

# FortiOS - CLI Reference

VERSION 5.4.8



## **FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

## **FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

## **FORTIGUARD CENTER**

<http://www.fortiguard.com>

## **FORTICAST**

<http://forticast.fortinet.com>

## **END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

## **FORTINET PRIVACY POLICY**

<https://www.fortinet.com/corporate/about-us/privacy.html>

## **FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



January 26, 2018

FortiOS - CLI Reference

01-548-99686-20180126

# TABLE OF CONTENTS

<b>Change Log</b>	<b>12</b>
<b>Introduction</b>	<b>13</b>
How this guide is organized	13
Availability of commands and options	13
<b>Managing Firmware with the FortiGate BIOS</b>	<b>15</b>
Accessing the BIOS	15
Navigating the menu	15
Loading firmware	15
Configuring TFTP parameters	16
Initiating TFTP firmware transfer	16
Booting the backup firmware	17
<b>Using the CLI</b>	<b>18</b>
Connecting to the CLI	18
Connecting to the CLI using a local console	18
Enabling access to the CLI through the network (SSH or Telnet)	19
Connecting to the CLI using SSH	20
Connecting to the CLI using Telnet	21
Command syntax	22
Terminology	22
Indentation	23
Notation	23
Sub-commands	25
Example of table commands	27
Permissions	29
Tips	29
<b>config</b>	<b>38</b>
antivirus	40
antivirus heuristic	40
antivirus profile	41
antivirus quarantine	43
antivirus settings	45
application	46
application casi profile	46
application custom	47

application internet-service-custom .....	47
application list .....	48
application name .....	51
application rule-settings .....	51
dlp .....	51
dlp filepattern .....	52
dlp fp-doc-source .....	53
dlp fp-sensitivity .....	54
dlp sensor .....	55
dlp settings .....	57
endpoint-control .....	58
endpoint-control forticlient-registration-sync .....	58
endpoint-control profile .....	58
endpoint-control settings .....	58
firewall .....	58
firewall address   address6 .....	58
firewall addrgrp   addgrp6 .....	67
firewall policy   policy6 .....	71
firewall schedule group .....	99
firewall schedule onetime .....	101
firewall service category .....	103
firewall service custom .....	105
firewall vip .....	113
ips .....	126
ips custom .....	126
ips global .....	128
ips rule .....	130
ips sensor .....	132
log .....	134
log custom-field .....	134
log eventfilter .....	134
log gui-display .....	136
log threat-weight .....	136
system .....	138
system admin .....	139
system central-management .....	142
system csf .....	144
system dhcp_server .....	145
system dns .....	149
system global .....	150
reset-sessionless-tcp {enable   disable} .....	162
system ha .....	167

system ha-monitor.....	181
system interface.....	182
l2forward {enable   disable}.....	186
system link-monitor.....	199
system np6.....	201
system npu.....	205
system password-policy.....	206
system sms-server.....	207
system wccp.....	207
Router mode.....	208
Client mode.....	209
user.....	210
user adgrp.....	210
user device.....	211
user device-access-list.....	212
user device-category.....	213
user device-group.....	213
user fortitoken.....	214
user fsso.....	214
user fsso-polling.....	215
user group.....	216
user krb-keytab.....	219
user ldap.....	220
user local.....	223
user password-policy.....	225
user peer.....	226
user peergrp.....	228
user pop3.....	228
user radius.....	228
user security-exempt-list.....	234
user setting.....	234
user tacacs+.....	237
vpn.....	238
vpn certificate.....	238
vpn ssl.....	269
wanopt.....	285
wanopt auth-group.....	285
auth-method {cert   psk}.....	285
wanopt peer.....	286
wanopt profile.....	287
wanopt settings.....	290
wanopt storage.....	290

wanopt webcache.....	291
web-proxy.....	293
web-proxy debug-url.....	293
web-proxy explicit.....	294
web-proxy forward-server.....	297
web-proxy forward-server-group.....	298
web-proxy global.....	299
web-proxy profile.....	301
web-proxy url-match.....	302
web-proxy wisp.....	303
wireless-controller.....	303
wireless-controller ap-status.....	303
wireless-controller global.....	304
wireless-controller setting.....	306
wireless-controller timers.....	306
wireless-controller vap.....	307
eap-reauth {enable   disable}.....	313
wireless-controller vap-group.....	316
wireless-controller wids-profile.....	317
wireless-controller wtp.....	321
wireless-controller wtp-group.....	327
wireless-controller wtp-profile.....	328
<b>execute.....</b>	<b>337</b>
backup.....	337
batch.....	340
bypass-mode.....	341
carrier-license.....	341
central-mgmt.....	341
cfg reload.....	342
cfg save.....	343
clear system arp table.....	343
cli check-template-status.....	343
cli status-msg-only.....	344
client-reputation.....	344
date.....	344
disk.....	345
disk raid.....	346
disk scan.....	347
dhcp lease-clear.....	347
dhcp lease-list.....	347
disconnect-admin-session.....	348
enter.....	348

erase-disk .....	348
factoryreset .....	349
factoryreset2 .....	349
formatlogdisk .....	349
forticarrier-license .....	349
forticlient .....	349
FortiClient-NAC .....	350
fortiguard-log .....	350
fortitoken .....	351
fortitoken-mobile .....	352
fsso refresh .....	352
ha disconnect .....	352
ha ignore-hardware-revision .....	353
ha manage .....	353
ha synchronize .....	354
interface dhcpclient-renew .....	355
interface pppoe-reconnect .....	355
log backup .....	355
log client-reputation-report .....	355
log convert-oldlogs .....	357
log delete-all .....	357
log delete-oldlogs .....	357
log detail .....	357
log display .....	358
log downgrade-log .....	358
log filter .....	358
log fortianalyzer test-connectivity .....	359
log list .....	360
log rebuild-sqldb .....	360
log recreate-sqldb .....	361
log-report reset .....	361
log restore .....	361
log roll .....	361
log shift-time .....	362
log upload-progress .....	362
modem dial .....	362
modem hangup .....	362
modem trigger .....	362
mrouter clear .....	363
netscan .....	363
pbx .....	364
ping .....	366

ping-options, ping6-options.....	366
ping6.....	368
policy-packet-capture delete-all.....	368
reboot.....	368
report.....	369
report-config reset.....	369
restore.....	369
revision.....	373
router clear bfd session.....	374
router clear bgp.....	374
router clear ospf process.....	375
router restart.....	375
send-fds-statistics.....	375
sensor detail.....	376
sensor list.....	376
set system session filter.....	377
set-next-reboot.....	379
sfp-mode-sgmii.....	379
shutdown.....	379
ssh.....	380
sync-session.....	380
system custom-language import.....	380
system fortisandbox test-connectivity.....	381
tac report.....	381
telnet.....	381
time.....	381
traceroute.....	382
tracert6.....	382
update-av.....	383
update-geo-ip.....	383
update-ips.....	383
update-list.....	384
update-now.....	384
update-src-vis.....	384
upd-vd-license.....	384
upload.....	385
usb-device.....	385
usb-disk.....	386
vpn certificate ca.....	386
vpn certificate crl.....	387
vpn certificate local export.....	388
vpn certificate local generate.....	389



vpn certificate local import .....	391
vpn certificate remote .....	392
vpn ipsec tunnel down .....	392
vpn ipsec tunnel up .....	393
vpn sslvpn del-all .....	393
vpn sslvpn del-tunnel .....	393
vpn sslvpn del-web .....	393
vpn sslvpn list .....	394
webfilter quota-reset .....	394
wireless-controller delete-wtp-image .....	394
wireless-controller list-wtp-image .....	394
wireless-controller reset-wtp .....	395
wireless-controller restart-acd .....	395
wireless-controller restart-wtpd .....	395
wireless-controller upload-wtp-image .....	395
<b>get .....</b>	<b>396</b>
application internet-service status .....	396
application internet-service-summary .....	396
certificate .....	396
extender modem-status .....	397
extender sys-info .....	398
firewall dnstranslation .....	398
firewall iprope appctrl .....	398
firewall iprope list .....	398
firewall proute, proute6 .....	399
firewall service custom .....	399
firewall shaper .....	400
grep .....	401
gui console status .....	401
hardware cpu .....	402
hardware memory .....	403
hardware nic .....	403
hardware npu .....	404
hardware status .....	407
ips decoder status .....	407
ips rule status .....	408
ips session .....	408
ips view-map .....	409
ipsec tunnel .....	409
mgmt-data status .....	410
pbx branch-office .....	410
pbx dialplan .....	410

pbx did .....	411
pbx extension .....	411
pbx ftgd-voice-pkg .....	411
pbx global .....	412
pbx ringgrp .....	412
pbx sip-trunk .....	413
pbx voice-menu .....	413
router info bfd neighbor .....	414
router info bgp .....	414
router info isis .....	416
router info kernel .....	416
router info multicast .....	417
router info ospf .....	418
router info protocols .....	420
router info rip .....	421
router info routing-table .....	421
router info vrrp .....	422
router info6 bgp .....	422
router info6 interface .....	423
router info6 kernel .....	424
router info6 ospf .....	424
router info6 protocols .....	424
router info6 rip .....	424
router info6 routing-table .....	425
switch-controller poe .....	425
system admin list .....	425
system admin status .....	426
system arp .....	427
system auto-update .....	427
system central-management .....	427
system checksum .....	428
system cmdb status .....	428
system fortianalyzer-connectivity .....	429
system fortiguard-log-service status .....	429
system fortiguard-service status .....	430
system ha-nonsync-csum .....	430
system ha status .....	430
system info admin status .....	433
system info admin ssh .....	434
system interface physical .....	434
system ip-conflict status .....	435
system mgmt-csum .....	435

system performance firewall .....	435
system performance status .....	436
system performance top .....	437
system session list .....	438
system session status .....	439
system session-helper-info list .....	439
system session-info .....	440
system source-ip .....	441
system startup-error-log .....	442
system stp list .....	442
system status .....	442
test .....	443
user adgrp .....	445
vpn certificate .....	445
vpn ike gateway .....	446
vpn ipsec tunnel details .....	446
vpn ipsec tunnel name .....	446
vpn ipsec tunnel summary .....	446
vpn ipsec stats crypto .....	446
vpn ipsec stats tunnel .....	447
vpn ssl monitor .....	447
vpn status l2tp .....	448
vpn status pptp .....	448
vpn status ssl .....	448
webfilter categories .....	448
webfilter ftgd-statistics .....	449
webfilter status .....	451
wireless-controller client-info .....	451
wireless-controller rf-analysis .....	451
wireless-controller scan .....	452
wireless-controller spectral-info .....	452
wireless-controller status .....	453
wireless-controller vap-status .....	453
wireless-controller wlchanlistlic .....	453
wireless-controller wtp-status .....	455
<b>tree .....</b>	<b>457</b>

## Change Log

Date	Change Description
January 26, 2018	Updated to FortiOS 5.4.8.
September 19, 2017	<p>The following changes have been made under <code>config system interface</code>:</p> <ul style="list-style-type: none"><li>• Added sub-command <code>priority-override</code>.</li><li>• Modified sub-command <code>switch-controller-access-vlan</code> to match FortiSwitch's similar CLI command, in order to aid in debugging and to avoid FortiLink incompatibility between FortiOS and FortiSwitch.</li></ul>
May 3, 2017	Initial release of new revision.

# Introduction

This document describes FortiOS 5.4 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI).

This document is a work in progress and is not complete. Our focus is on documenting the most commonly used CLI commands or the commands that require more explanation. Now that we have published the first version you can expect to see updates as more commands and more features are added to the document. We will also have an HTML version up soon and all of this information will be accessible from <http://cli.fortinet.com>.

If you have comments on this content or requests for commands that are not included contact us at [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## How this guide is organized

This document contains the following sections:

[Managing Firmware with the FortiGate BIOS](#) describes how to change firmware at the console during FortiGate unit boot-up.

[Using the CLI](#) describes how to connect to the CLI and some basics of how it works.

[config](#) describes the commands for each configuration branch of the FortiOS CLI. This section is a work in progress with more content to be added in future versions.

[execute](#) describes execute commands.

[get](#) describes get commands.

[tree](#) describes the tree command.

## Availability of commands and options

Some FortiOS™ CLI commands and options are not available on all FortiGate units. The CLI displays an error message if you attempt to enter a command or option that is not available. You can use the question mark '?' to verify the commands and options that are available.

Commands and options may not be available for the following reasons:

### FortiGate model

All commands are not available on all FortiGate models. For example, low-end FortiGate models do not support the aggregate interface type option of the `config system interface` command.

### Hardware configuration

For example, some AMC module commands are only available when an AMC module is installed.

**FortiOS Carrier, FortiGate Voice, FortiWiFi, etc**

Commands for extended functionality are not available on all FortiGate models. The CLI Reference includes commands only available for FortiWiFi units, FortiOS Carrier, and FortiGate Voice units.

# Managing Firmware with the FortiGate BIOS

FortiGate units are shipped with firmware installed. Usually firmware upgrades are performed through the web-based manager or by using the CLI `execute restore` command. From the console, you can also interrupt the FortiGate unit's boot-up process to load firmware using the BIOS firmware that is a permanent part of the unit.

Using the BIOS, you can:

- view system information
- format the boot device
- load firmware and reboot
- reboot the FortiGate unit from the backup firmware, which then becomes the default firmware

## Accessing the BIOS

The BIOS menu is available only through direct connection to the FortiGate unit's Console port. During boot-up, "Press any key" appears briefly. If you press any keyboard key at this time, boot-up is suspended and the BIOS menu appears. If you are too late, the boot-up process continues as usual.

## Navigating the menu

The main BIOS menu looks like this:

```
[C]: Configure TFTP parameters
[R]: Review TFTP parameters
[T]: Initiate TFTP firmware transfer
[F]: Format boot device
[Q]: Quit menu and continue to boot
[I]: System Information
[B]: Boot with backup firmware and set as default
[Q]: Quit menu and continue to boot
[H]: Display this list of options
```

Enter C,R,T,F,I,B,Q, or H:

Typing the bracketed letter selects the option. Input is case-sensitive. Most options present a submenu. An option value in square brackets at the end of the "Enter" line is the default value which you can enter simply by pressing Return. For example,

Enter image download port number [WAN1]:

In most menus, typing H re-lists the menu options and typing Q returns to the previous menu.

## Loading firmware

The BIOS can download firmware from a TFTP server that is reachable from a FortiGate unit network interface. You need to know the IP address of the server and the name of the firmware file to download.

The downloaded firmware can be saved as either the default or backup firmware. It is also possible to boot the downloaded firmware without saving it.

## Configuring TFTP parameters

Starting from the main BIOS menu

```
[C]: Configure TFTP parameters.
```

### Selecting the VLAN (if VLANs are used)

```
[V]: Set local VLAN ID.
```

### Choose port and whether to use DHCP

```
[P]: Set firmware download port.
```

The options listed depend on the FortiGate model. Choose the network interface through which the TFTP server can be reached. For example:

```
[0]: Any of port 1 - 7
[1]: WAN1
[2]: WAN2
Enter image download port number [WAN1]:
[D]: Set DHCP mode.
Please select DHCP setting
[1]: Enable DHCP
[2]: Disable DHCP
```

If there is a DHCP server on the network, select [1]. This simplifies configuration. Otherwise, select [2].

### Non-DHCP steps

```
[I]: Set local IP address.
Enter local IP address [192.168.1.188]:
```

This is a temporary IP address for the FortiGate unit network interface. Use a unique address on the same subnet to which the network interface connects.

```
[S]: Set local subnet mask.
Enter local subnet mask [255.255.252.0]:
[G]: Set local gateway.
```

The local gateway IP address is needed if the TFTP server is on a different subnet than the one to which the FortiGate unit is connected.

### TFTP and filename

```
[T]: Set remote TFTP server IP address.
Enter remote TFTP server IP address [192.168.1.145]:
[F]: Set firmware file name.
Enter firmware file name [image.out]:
```

Enter [Q] to return to the main menu.

## Initiating TFTP firmware transfer

Starting from the main BIOS menu

```
[T]: Initiate TFTP firmware transfer.
```



```
Please connect TFTP server to Ethernet port 'WAN1'.
```

```
MAC: 00:09:0f:b5:55:28
```

```
Connect to tftp server 192.168.1.145 ...
```

```
#####
Image Received.
Checking image... OK
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
```

After you choose any option, the FortiGate unit reboots. If you choose [D] or [B], there is first a pause while the firmware is copied:

```
Programming the boot device now.
.....
.....
```

## Booting the backup firmware

You can reboot the FortiGate unit from the backup firmware, which then becomes the default firmware.

Starting from the main BIOS menu

```
[B]: Boot with backup firmware and set as default.
```

If the boot device contains backup firmware, the FortiGate unit reboots. Otherwise the unit responds:

```
Failed to mount filesystem. . .
Mount back up partition failed.
Back up image open failed.
Press 'Y' or 'y' to boot default image.
```

# Using the CLI

The command line interface (CLI) is an alternative configuration tool to the web-based manager. While the configuration of the GUI uses a point-and-click method, the CLI requires typing commands or uploading batches of commands from a text file, like a configuration script.

This section also explains common CLI tasks that an administrator does on a regular basis and includes the topics:

- [Connecting to the CLI](#)
- [Command syntax](#)
- [Sub-commands](#)
- [Permissions](#)
- [Tips](#)

## Connecting to the CLI

You can access the CLI in three ways:

- [Locally with a console cable](#) — Connect your computer directly to the FortiGate unit's console port. Local access is required in some cases:
  - If you are installing your FortiGate unit for the first time and it is not yet configured to connect to your network, you may only be able to connect to the CLI using a local serial console connection, unless you reconfigure your computer's network settings for a peer connection.
  - Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until after the boot process has completed, making local CLI access the only viable option.
- [Through the network](#) — Connect your computer through any network attached to one of the FortiGate unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect using the **CLI Console** widget in the web-based manager.
- [Locally with FortiExplorer](#) — Connect your computer directly to the FortiGate unit's USB management port. FortiExplorer provides direct access to the FortiOS setup wizard, Web-based Manager, and CLI console.

## Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port. To connect to the local console you need:

- A computer with an available serial communications (COM) port.
- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package.
- Terminal emulation software such as HyperTerminal for Microsoft Windows.

The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

**To connect to the CLI using a local serial console connection**

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start HyperTerminal.
3. For the **Connection Description**, enter a **Name** for the connection, and select **OK**.
4. On the **Connect using** drop-down list box, select the communications (COM) port on your management computer you are using to connect to the FortiGate unit.
5. Select **OK**.
6. Select the following **Port** settings and select **OK**.

<b>Bits per second</b>	9600
<b>Data bits</b>	8
<b>Parity</b>	None
<b>Stop bits</b>	1
<b>Flow control</b>	None

7. Press **Enter** or **Return** on your keyboard to connect to the CLI.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

The CLI displays the following text:

```
Welcome!  
Type ? to list available commands.
```

You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet.

**Enabling access to the CLI through the network (SSH or Telnet)**

SSH or Telnet access to the CLI is accomplished by connecting your computer to the FortiGate unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.



If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the **CLI Console** widget in the web-based manager.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is not connected directly or through a switch, you must also configure the FortiGate unit with a static route to a router that can forward packets from the FortiGate unit to your computer. You can do this using either a local console connection or the web-based manager.

**Requirements**

- A computer with an available serial communications (COM) port and RJ-45 port
- Terminal emulation software such as HyperTerminal for Microsoft Windows

- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- A network cable
- Prior configuration of the operating mode, network interface, and static route.

### To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiGate unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI.
4. Enter the following command:

```
config system interface
  edit <interface_str>
    set allowaccess <protocols_list>
  end
```

where:

- **<interface\_str>** is the name of the network interface associated with the physical network port and containing its number, such as `port1`
- **<protocols\_list>** is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
config system interface
  edit port1
    set allowaccess ssh telnet
  end
```

5. To confirm the configuration, enter the command to display the network interface's settings.

```
show system interface <interface_str>
```

The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

## Connecting to the CLI using SSH

Once the FortiGate unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. FortiGate units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. The following procedure uses PuTTY. Steps may vary with other SSH clients.

### To connect to the CLI using SSH

1. On your management computer, start an SSH client.
2. In **Host Name (or IP Address)**, enter the IP address of a network interface on which you have enabled SSH administrative access.
3. In **Port**, enter `22`.

4. For the **Connection type**, select **SSH**.

5. Select **Open**.

The SSH client connects to the FortiGate unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiGate unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiGate unit but used a different IP address or SSH key. This is normal. If your management computer is directly connected to the FortiGate unit with no network hosts between them.

6. Click **Yes** to verify the fingerprint and accept the FortiGate unit's SSH key. You will not be able to log in until you have accepted the key.
7. The CLI displays a login prompt.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for this administrator account and press Enter.

The FortiGate unit displays a command prompt (its host name followed by a #). You can now enter CLI commands.



If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

---

## Connecting to the CLI using Telnet

Once the FortiGate unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.



Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

---

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept Telnet connections.

### To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiGate network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.
4. Type the password for this administrator account and press Enter.

The FortiGate unit displays a command prompt (its host name followed by a #). You can now enter CLI commands.



If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

---

## Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the conventions below to describe valid command syntax.

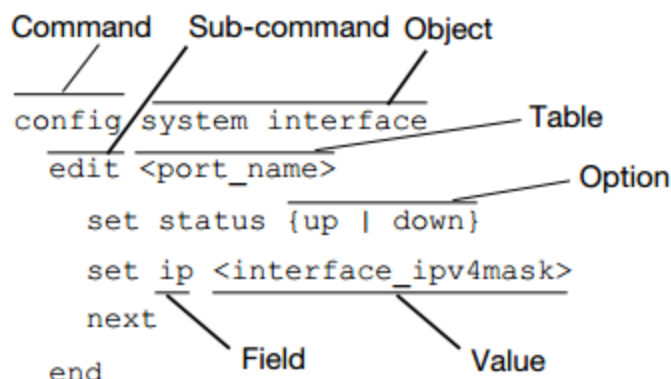
## Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

### Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiGate unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multiline command lines, which can be entered using an escape sequence. Valid command lines must be unambiguous if abbreviated. Optional words or other command line permutations are indicated by syntax notation.
- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands. Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope.
- **object** — A part of the configuration that contains tables and / or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them.

- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiGate unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation.
- **option** — A kind of value that must be one or more words from of a fixed set of options.

## Indentation

Indentation indicates levels of nested commands, which indicate what other sub-commands are available from within the scope. For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
  end
```

## Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

### Command syntax notation

Convention	Description
<b>Square brackets</b> [ ]	A non-required word or series of words. For example:  <code>[verbose {1   2   3}]</code>  indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as <code>verbose 3</code> .

Convention	Description
<b>Angle brackets</b> < >	<p>A word constrained by data type. The angled brackets contain a descriptive name followed by an underscore ( _ ) and suffix that indicates the valid data type. For example, &lt;retries_int&gt;, indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> <li>• &lt;xxx_name&gt;: A name referring to another part of the configuration, such as policy_A.</li> <li>• &lt;xxx_index&gt;: An index number referring to another part of the configuration, such as 0 for the first static route.</li> <li>• &lt;xxx_pattern&gt;: A regular expression or word with wild cards that matches possible variations, such as *@example.com to match all email addresses ending in @example.com.</li> <li>• &lt;xxx_fqdn&gt;: A fully qualified domain name (FQDN), such as mail.example.com.</li> <li>• &lt;xxx_email&gt;: An email address, such as admin@example.com.</li> <li>• &lt;xxx_ipv4&gt;: An IPv4 address, such as 192.168.1.99.</li> <li>• &lt;xxx_v4mask&gt;: A dotted decimal IPv4 netmask, such as 255.255.255.0.</li> <li>• &lt;xxx_ipv4mask&gt;: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.</li> <li>• &lt;xxx_ipv4/mask&gt;: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.1/24</li> <li>• &lt;xxx_ipv4range&gt; : A hyphen ( - )-delimited inclusive range of IPv4 addresses, such as 192.168.1.1-192.168.1.255.</li> <li>• &lt;xxx_ipv6&gt;: A colon ( : )-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.</li> <li>• &lt;xxx_v6mask&gt;: An IPv6 netmask, such as /96.</li> </ul>
	<ul style="list-style-type: none"> <li>• &lt;xxx_ipv6mask&gt;: A dotted decimal IPv6 address and netmask separated by a space.</li> <li>• &lt;xxx_str&gt;: A string of characters that is not another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.</li> <li>• &lt;xxx_int&gt;: An integer number that is <b>not</b> another data type, such as 15 for the number of minutes.</li> </ul>
<b>Curly braces</b> { }	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].</p>



Convention	Description
<b>Options delimited by vertical bars  </b>	<p>Mutually exclusive options. For example:</p> <pre>{enable   disable}</pre> <p>indicates that you must enter either <code>enable</code> or <code>disable</code>, but must not enter both.</p>
<b>Options delimited by spaces</b>	<p>Non-mutually exclusive options. For example:</p> <pre>{http https ping snmp ssh telnet}</pre> <p>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:</p> <pre>ping https ssh</pre>

## Sub-commands

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands. When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin) #
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
  next
end
```

Sub-command scope is indicated by indentation.

Available sub-commands vary by command. From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

## Commands for tables

### clone <table>

Clone (or make a copy of) a table from the current object.

For example, in `config firewall policy`, you could enter the following command to clone security policy 27 to create security policy 30:

```
clone 27 to 30
```

In `config antivirus profile`, you could enter the following command to clone an antivirus profile named `av_pro_1` to create a new antivirus profile named `av_pro_2`:

```
clone av_pro_1 to av_pro_2
```

`clone` may not be available for all tables.

### delete <table>

Remove a table from the current object.

For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s first-name and email-address.

`delete` is only available within objects containing tables.

### edit <table>

Create or edit a table in the current object.

For example, in `config system admin`:

- edit the settings for the default `admin` administrator account by typing `edit admin`.
- add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`.

`edit` is an interactive sub-command: further sub-commands are available from within `edit`.

`edit` changes the prompt to reflect the table you are currently editing.

`edit` is only available within objects containing tables.

In objects such as security policies, `<table>` is a sequence number. To create a new entry without the risk of overwriting an existing one, enter `edit 0`. The CLI initially confirms the creation of entry 0, but assigns the next unused number after you finish editing and enter `end`.

### end

Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.

<b>get</b>	<p>List the configuration of the current object or table.</p> <ul style="list-style-type: none"> <li>• In objects, <code>get</code> lists the table names (if present), or fields and their values.</li> <li>• In a table, <code>get</code> lists the fields and their values.</li> </ul> <p>For more information on <code>get</code> commands, see the <a href="#">CLI Reference</a>.</p>
<b>purge</b>	<p>Remove all tables in the current object.</p> <p>For example, in <code>config user local</code>, you could type <code>get</code> to see the list of user names, then type <code>purge</code> and then <code>y</code> to confirm that you want to delete all users.</p> <p><code>purge</code> is only available for objects containing tables.</p> <p><b>Caution:</b> Back up the FortiGate unit before performing a <code>purge</code>. <code>purge</code> cannot be undone. To restore purged tables, the configuration must be restored from a backup.</p> <p><b>Caution:</b> Do not purge <code>system interface</code> or <code>system admin</code> tables. <code>purge</code> does not provide default tables. This can result in being unable to connect or log in, requiring the FortiGate unit to be formatted and restored.</p>
<b>rename &lt;table&gt; to &lt;table&gt;</b>	<p>Rename a table.</p> <p>For example, in <code>config system admin</code>, you could rename <code>admin3</code> to <code>fwadmin</code> by typing <code>rename admin3 to fwadmin</code>.</p> <p><code>rename</code> is only available within objects containing tables.</p>
<b>show</b>	<p>Display changes to the default configuration. Changes are listed in the form of configuration commands.</p>

## Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1) #
```

### Commands for fields

<b>abort</b>	Exit both the <code>edit</code> and/or <code>config</code> commands without saving the fields.
--------------	--

<b>append</b>	Add an option to an existing list.
<b>end</b>	Save the changes made to the current table or object fields, and exit the <code>config</code> command. (To exit without saving, use <code>abort</code> instead.)
<b>get</b>	<p>List the configuration of the current object or table.</p> <ul style="list-style-type: none"> <li>• In objects, <code>get</code> lists the table names (if present), or fields and their values.</li> <li>• In a table, <code>get</code> lists the fields and their values.</li> </ul>
<b>move</b>	Move an object within a list, when list order is important. For example, rearranging security policies within the policy list.
<b>next</b>	<p>Save the changes you have made in the current table's fields, and exit the <code>edit</code> command to the object prompt. (To save and exit completely to the root prompt, use <code>end</code> instead.)</p> <p><code>next</code> is useful when you want to create or edit several tables in the same object, without leaving and re-entering the <code>config</code> command each time.</p> <p><code>next</code> is only available from a table prompt; it is not available from an object prompt.</p>
<b>select</b>	<p>Clear all options except for those specified.</p> <p>For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command <code>select member B</code>.</p>
<b>set &lt;field&gt; &lt;value&gt;</b>	<p>Set a field's value.</p> <p>For example, in <code>config system admin</code>, after typing <code>edit admin</code>, you could type <code>set password newpass</code> to change the password of the <code>admin</code> administrator to <code>newpass</code>.</p> <p><b>Note:</b> When using <code>set</code> to change a field containing a space-delimited list, type the whole new list. For example, <code>set &lt;field&gt; &lt;new-value&gt;</code> will replace the list with the <code>&lt;new-value&gt;</code> rather than appending <code>&lt;new-value&gt;</code> to the list.</p>
<b>show</b>	Display changes to the default configuration. Changes are listed in the form of configuration commands.
<b>unselect</b>	Remove an option from an existing list.
<b>unset &lt;field&gt;</b>	<p>Reset the table or object's fields to default values.</p> <p>For example, in <code>config system admin</code>, after typing <code>edit admin</code>, typing <code>unset password</code> resets the password of the <code>admin</code> administrator account to the default (in this case, no password).</p>

### Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

## Permissions

Access profiles control which CLI commands an administrator account can access. Access profiles assign either read, write, or no access to each area of the FortiGate software. To view configurations, you must have read access. To make changes, you must have write access. So, depending on the account used to log in to the FortiGate unit, you may not have complete access to all CLI commands

Unlike other administrator accounts, the `admin` administrator account exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing **all** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.



Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiGate unit.

For complete access to all commands, you must log in with the administrator account named `admin`.

## Tips

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

## Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

## Shortcuts and key commands

### Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words.	?
If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	
Complete the word with the next available match.	Tab
Press the key multiple times to cycle through available matches.	
Recall the previous command.	Up arrow, or Ctrl + P
Command memory is limited to the current session.	
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines.	Ctrl + C
If you are not currently within an interactive command such as <code>config</code> or <code>edit</code> , this closes the CLI connection.	
Continue typing a command on the next line for a multi-line command.	
For each line that you want to continue, terminate it with a backslash (\). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

## Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy stat`.

## Adding and removing options from lists

When adding options to a list, such as a user group, using the `set` command will remove the previous configuration. For example, if you wish to add user D to a user group that already contains members A, B, and C, the command would need to be `set member A B C D`. If only `set member D` was used, then all former members would be removed from the group.

However, there are additional commands which can be used instead of `set` for changing options in a list.

### Additional commands for lists

<b>append</b>	Add an option to an existing list.  For example, <code>append member</code> would add user D to a user group while all previous group members are retained
<b>select</b>	Clear all options except for those specified.  For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command <code>select member B</code> .
<b>unselect</b>	Remove an option from an existing list.  For example, <code>unselect member A</code> would remove member A from a group while all previous group members are retained.

## Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

### Environment variables

<b>\$USERFROM</b>	The management access type ( <code>ssh</code> , <code>telnet</code> , <code>jsconsole</code> for the <b>CLI Console</b> widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
<b>\$USERNAME</b>	The account name of the administrator that configured the item.
<b>\$SerialNum</b>	The serial number of the FortiGate unit.

For example, the FortiGate unit's host name can be set to its serial number.

```
config system global
    set hostname $SerialNum
end
```

## Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields. These characters are special characters, also known as reserved characters.

You may be able to enter special character as part of a string's value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\) character.

In other cases, different keystrokes are required to input a special character. If you need to enter ? as part of config, you first need to input CTRL-V. If you enter the question mark (?) without first using CTRL-V, the question mark has a different meaning in CLI: it will show available command options in that section.

For example, if you enter ? without CTRL-V:

```
edit "*.xe
token line: Unmatched double quote.
```

If you enter ? with CTRL-V:

```
edit "*.xe?"
new entry '*.xe?' added
```

### Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: "Security Administrator".  Enclose the string in single quotes: 'Security Administrator'.  Precede the space with a backslash: Security\ Administrator.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\



## Using grep to filter get and show command output

In many cases, the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large `get` or `show` command output, you can use the `grep` command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX `grep`, used for searching text output based on regular expressions.

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr           00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
```

Use the following command to display all lines in HTTP replacement message commands that contain URL (upper or lower case):

```
show system replacemsg http | grep -i url
```

There are three additional options that can be applied to `grep`:

```
-A <num> After
-B <num> Before
-C <num> Context
```

The option `-f` is also available to support Fortinet contextual output, in order to show the complete configuration. The following example shows the difference in output when `-f` option is used versus when it is not.

### Using -f:

```
show | grep -f ldap-group1
config user group
  edit "ldap-group1"
    set member "pc40-LDAP"
  next
end
config firewall policy
  edit 2
    set srcintf "port31"
    set dstintf "port32"
    set srcaddr "all"
    set action accept
    set identity-based enable
    set nat enable
    config identity-based-policy
      edit 1
        set schedule "always"
        set groups "ldap-group1"
        set dstaddr "all"
        set service "ALL"
      next
    end
  next
end
```

**Without using -f:**

```
show | grep ldap-group1
edit "ldap-group1"
set groups "ldap-group1"
```

## Language support and regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice. To use other languages in those cases, you must use the correct encoding.

Input is stored using Unicode UTF-8 encoding but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes ( \ ) could be inadvertently interpreted as the symbol for the Japanese yen ( ¥ ) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.



HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

If you configure your FortiGate unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

If you choose to configure parts of the FortiGate unit using non-ASCII characters, verify that all systems interacting with the FortiGate unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

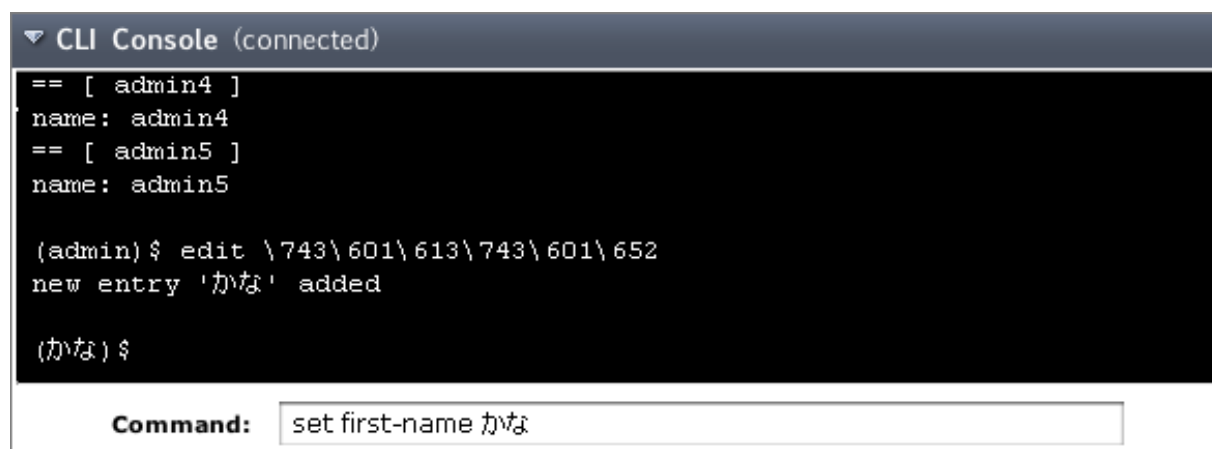
Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web-based manager or CLI. Exceptions

include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiGate unit receives.

### To enter non-ASCII characters in the CLI Console widget

1. On your management computer, start your web browser and go to the URL for the FortiGate unit's web-based manager.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiGate unit.
4. Go to **System > Dashboard > Status**.
5. In title bar of the **CLI Console** widget, click **Edit** (the pencil icon).
6. Enable **Use external command input box**.
7. Select **OK**.
8. The **Command** field appears below the usual input and display area of the **CLI Console** widget.
9. In **Command**, type a command.

### Entering encoded characters (CLI Console widget):



10. Press **Enter**.

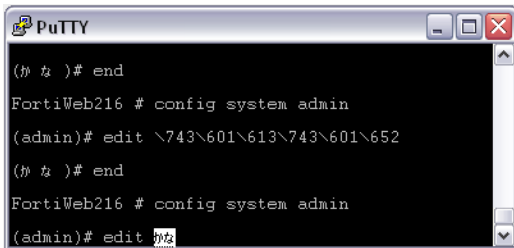
In the display area, the **CLI Console** widget displays your previous command interpreted into its character code equivalent, such as:

```
edit \743\601\613\743\601\652  
and the command's output.
```

### To enter non-ASCII characters in a Telnet/SSH client

1. On your management computer, start your Telnet or SSH client.
2. Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding.  
Support for sending and receiving international characters varies by each Telnet/SSH client. Consult the documentation for your Telnet/SSH client.
3. Log in to the FortiGate unit.
4. At the command prompt, type your command and press Enter.

### Entering encoded characters (PuTTY):



You may need to surround words that use encoded characters with single quotes ( ' ).

Depending on your Telnet/SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5. The CLI displays your previous command and its output.

## Screen paging

You can configure the CLI to pause after displaying each page's worth of text when displaying multiple pages of output. When the display pauses, the last line displays `--More--`. You can then either:

- press the spacebar to display the next page.
- type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
  set output more
end
```

## Baud rate

You can change the default baud rate of the local console connection.

To change the baud rate enter the following commands:

```
config system console
  set baudrate {115200 | 19200 | 38400 | 57600 | 9600}
end
```

## Editing the configuration file on an external host

You can edit the FortiGate configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiGate unit.

Editing the configuration on an external host can be timesaving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

### To edit the configuration on your computer

1. Use `execute backup` to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.



Do not edit the first line. The first line(s) of the configuration file (preceded by a # character) contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration file when you attempt to restore it.

---

3. Use `execute restore` to upload the modified configuration file back to the FortiGate unit.  
The FortiGate unit downloads the configuration file and checks that the model information is correct. If it is, the FortiGate unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiGate unit ignores the command. If the configuration file is valid, the FortiGate unit restarts and loads the new configuration.

# config

Use the config commands to change your FortiGate's configuration.

The command branches and commands are in alphabetical order. The information in this section has been extracted and formatted from FortiOS source code. The extracted information includes the command syntax, command descriptions (extracted from CLI help) and default values. This is the first version of this content produced in this way. You can send comments about this content to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

- antivirus
- antivirus heuristic
- antivirus profile
- antivirus quarantine
- antivirus settings
- application
- application casi profile
- application custom
- application internet-service-custom
- application list
- application name
- application rule-settings
- dlp
- dlp filepattern
- dlp fp-doc-source
- dlp fp-sensitivity
- dlp sensor
- dlp settings
- endpoint-control
- endpoint-control forticlient-registration-sync
- endpoint-control profile
- endpoint-control settings
- firewall
- firewall address | address6
- firewall addrgrp | addgrp6
- firewall policy | policy6
- firewall schedule group
- firewall schedule onetime
- firewall service category
- firewall service custom
- firewall vip
- ips
- ips custom
- ips global
- ips rule
- ips sensor

- log
- log custom-field
- log eventfilter
- log gui-display
- log threat-weight
- system
- system admin
- system central-management
- system csf
- system dhcp\_server
- system dns
- system global
- reset-sessionless-tcp {enable | disable}
- system ha
- system ha-monitor
- system interface
- system link-monitor
- system np6
- system npu
- system password-policy
- system sms-server
- system wccp
- Router mode
- Client mode
- user
- user adgrp
- user device
- user device-access-list
- user device-category
- user device-group
- user fortitoken
- user fsso
- user fsso-polling
- user group
- user krb-keytab
- user ldap
- user local
- user password-policy
- user peer
- user peergrp
- user pop3
- user radius
- user security-exempt-list
- user setting
- user tacacs+

- vpn
- vpn certificate
- vpn ssl
- wanopt
- wanopt auth-group
- auth-method {cert | psk}
- wanopt peer
- wanopt profile
- wanopt settings
- wanopt storage
- wanopt webcache
- web-proxy
- web-proxy debug-url
- web-proxy explicit
- web-proxy forward-server
- web-proxy forward-server-group
- web-proxy global
- web-proxy profile
- web-proxy url-match
- web-proxy wisp
- wireless-controller
- wireless-controller ap-status
- wireless-controller global
- wireless-controller setting
- wireless-controller timers
- wireless-controller vap
- eap-reauth {enable | disable}
- wireless-controller vap-group
- wireless-controller wids-profile
- wireless-controller wtp
- wireless-controller wtp-group
- wireless-controller wtp-profile

## antivirus

Use antivirus commands to configure antivirus scanning for services, quarantine options, and to enable or disable grayware and heuristic scanning.

This section includes descriptions for the following commands:

### antivirus heuristic

Configure the global heuristic options used for antivirus scanning.



### mode {pass | block | disable}

Select the mode to use for heuristics. The following options are available:

- `pass`: Enable heuristics but pass any detected files.
- `block`: Enable heuristics and block any detected files.
- `disable`: Turn off heuristics.

The default is `disable`.

## antivirus profile

Create and configure antivirus profiles that can be applied to firewall policies.

### comment <string>

Add a comment to the profile.

---

### replacemsg-group <group-name>

Set a replacement message group to use with antivirus scanning.

---

### inspection-mode {proxy | flow-based}

Set the inspection mode. Select between the following options:

- `proxy`: Scanning reconstructs content passing through the FortiGate unit and inspects the content for security threats.
- `flow-based`: Scanning takes a snapshot of content packets and uses pattern matching to identify security threats in the content.

The default is `proxy`. For more information, see [Inspection Modes](#).

---

### ftgd-analytics {disable}

Choose which files are sent to FortiSandbox for further inspection. Select between the following options:

- `disable`: No files are sent for inspection.
- `suspicious`: Files that the antivirus engine deems suspicious as sent for inspection.
- `everything`: All files are sent for inspection.

The default is `disable`.

---

---

### **analytics-db {enable | disable}**

Enable or disable using antivirus signatures from the FortiSandbox's database as well as signatures from the FortiGate. Disabled by default.

---

### **mobile-malware-db {enable | disable}**

Enable or disable using antivirus signatures from the mobile malware signature database as well as signatures from the FortiGate. Enabled by default.

---

### **config {http | ftp | imap | pop3 | smtp | smb}**

Configure how this profile handles specific protocols.

#### **options {scan | avmonitor | quarantine}**

Set an action to apply to traffic using this protocol. Select from the following options:

- `scan`: Scan files transferred using this protocol for viruses.
- `avmonitor`: Log detected viruses, but allow them through the firewall without modification.
- `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGates with a hard disk or those connected to a FortiAnalyzer.

#### **archive-block {encrypted | corrupted | multipart | nested | mailbomb | unhandled}**

Set which types of archived files to block.

#### **archive-log {encrypted | corrupted | multipart | nested | mailbomb | unhandled}**

Set which types of archived files to log.

#### **emulator {enable | disable}**

Enable or disable the virus emulator. Enabled by default.

#### **executables {default | virus}**

Set how this profile treats executable files sent with this protocol. Select from the following options:

- `default`: Perform standard antivirus scanning.
- `virus`: Treat executable files as viruses.

The default option is `default`. This option is only available for IMAP, POP3, and SMTP.

---

### **config nac-quar**

Configure the quarantine settings for this profile.

### infected {none | quar-src-ip}

Set which infected hosts are added to the banned user list. Select from the following options:

- `none`: No hosts are banned.
- `quar-src-ip`: All traffic from the source IP is banned.

The default is `none`.

### expiry <duration>

Set the duration of the quarantine in the days, hours, minutes format `<###d##h##m>`. The default is 5 minutes. This option only appears if `infected` is set to `quar-src-ip`.

### log {enable | disable}

Enable or disable logging for antivirus quarantines. Disabled by default.

---

### av-virus-log {enable | disable}

Enable or disable logging for antivirus scanning. Enabled by default.

---

### av-block-log {enable | disable}

Enable or disable logging files that are blocked by antivirus. Enabled by default.

---

### scan-mode {quick | full}

Choose which scan mode to use for antivirus inspection. Select from the following options:

- `quick`: This mode uses a compact antivirus database and advanced techniques to improve performance.
- `full`: In this mode, content packets are buffered while simultaneously being sent to their destination.

The default is `full`. These options are only available when `inspection-mode` is set to `flow-based`.

## antivirus quarantine

Configure the antivirus quarantine options. **Note:** MM1, MM3, MM4, and MM7 traffic types supported only in FortiOS Carrier.

### agelimit <int>

Set the age limit for how long files are kept in quarantine. 0 means files are kept forever. The default is 0. This option appears when `destination` is not set to `NULL`.

---

---

**maxfilesize <int>**

Specify, in MB, the maximum file size to quarantine. 0 means unlimited. The default is 0.

---

**quarantine-quota <int>**

Set the antivirus quarantine quota in MB, which is the amount of disk space to reserve for quarantining files. 0 means unlimited. The default is 0.

---

**drop-infected {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}**

Drop infected files found in traffic for the specified protocols. By default, no files are dropped.

---

**store-infected {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}**

Quarantine virus infected files found in traffic for the specified protocols. By default, all protocols are specified.

---

**drop-blocked {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}**

Drop blocked files found in traffic for the specified protocols. By default, no files are dropped.

---

**store-blocked {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}**

Quarantine blocked files found in traffic for the specified protocols. By default, all protocols are specified.

---

**drop-heuristic {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}**

Drop files found by heuristic scanning in traffic for the specified protocols. By default, no files are dropped.

---

**store-heuristic {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}**

Quarantine files found by heuristic scanning in traffic for the specified protocols. By default, all protocols are specified.

---

### **drop-intercepted {imap | smtp | pop3 | http | ftp | mm1 | mm3 | mm4 | mm7}**

For FortiOS Carrier, drop intercepted files found in traffic for the specified protocols. By default, no files are dropped.

---

### **store-intercepted {imap | smtp | pop3 | http | ftp | mm1 | mm3 | mm4 | mm7}**

For FortiOS Carrier, quarantine intercepted files found in traffic for the specified protocols. By default, all protocols are specified.

---

### **lowspace {drop-new | ovrw-old}**

Select the method for handling additional quarantined files when the FortiGate hard disk is running out of space. Select from the following options:

- `drop-new`: Drop new quarantine files.
- `ovrw-old`: Overwrite the oldest file (lowest TTL).

The default is `ovrw-old`.

---

### **destination {NULL | disk | FortiAnalyzer}**

Set the destination where files are quarantined. Select from the following options:

- `NULL`: No files are quarantined.
- `disk`: Files are quarantined using the FortiGate's hard disk (if present).
- `FortiAnalyzer`: Files are quarantined using a FortiAnalyzer.

If the FortiGate has a hard disk, the default is `disk`. If no hard disk is available, the default is `NULL`.

## **antivirus settings**

Configure basic antivirus settings

### **default-db {normal | extended | extreme}**

Select the database to be used for antivirus scanning. Both proxy and flow inspection modes use these databases.

- `normal`: use the normal virus database, which includes viruses that are "in the wild," including the commonly seen viruses. For regular antivirus protection, it is sufficient to use this database.
- `extended`: use the extended virus database, which includes both "in the wild" viruses and a large collection of "in the zoo" viruses. It is suitable for an enhanced security environment.

- `extreme`: use the extreme virus database, which includes both "in the wild" viruses and all available "in the zoo" viruses. It is suitable for an enhanced security environment.

The default is `normal`.

---

## grayware {enable | disable}

Enable or disable the detection of grayware, including adware, dial, downloader, hacker tool, keylogger, RAT, and spyware. The is enabled by default.

## application

Use these commands to configure application control.

This section includes descriptions for the following commands:

## application casi profile

Configure a profile for Cloud Access Security Inspection (CASI).

### comment <string>

Add a comment to the CASI profile.

---

### replacemsg-group <group-name>

Set a replacement message group to use with CASI scanning.

---

### app-replacemsg {enable | disable}

Enable or disable replacement messages for blocked applications. Enabled by default.

---

## config entries

Configure application entries for scanning.

### application <ID>

Chose which application to apply the profile to. Type `set application ?` to view all available options.

### action {pass | block | reset}

Select the action to apply to this application's traffic. The default is `block`.

---

**log {enable | disable}**

Enable or disable logging of this application's traffic. Enabled by default.

## application custom

Configure a custom firewall application.

**comment <string>**

Add a comment to the custom application.

---

**signature <string>**

Set the application signature. For information about custom application signatures, see [Custom Application & IPS Signatures](#).

---

**category <ID>**

Set the category ID. Type `set category ?` to view all available options.

---

**protocol <ID>**

Set the protocol ID. Type `set protocol ?` to view all available options.

---

**technology <ID>**

Set the technology ID. Type `set technology ?` to view all available options.

---

**vendor <ID>**

Set the vendor ID. Type `set vendor ?` to view all available options.

## application internet-service-custom

Configure a custom Internet service application.

---

### master-service-id <ID>

Set the Internet service database application ID for the service. Type `set master-service-id ?` to view all available options.

---

### comment <string>

Add a comment to the service.

## application list

Configure an application control list.

### comment <string>

Add a comment to the control list.

---

### replacemsg-group <group-name>

Select a replacement message group to use for the control list.

---

### other-application-action {pass | block}

Set the action to take for traffic from other applications. The default is `pass`.

---

### app-replacemsg {enable | disable}

Enable or disable replacement messages for blocked application traffic. Default is `enable`.

---

### other-application-log {enable | disable}

Enable or disable logging traffic from other applications. Default is `disable`.

---

### unknown-application-action {pass | block}

Set an action to take for traffic from unknown applications. The default is `pass`.

---



### unknown-application-log {enable | disable}

Enable or disable logging traffic from unknown applications. Default is `disable`.

---

### p2p-black-list {skype | edonkey | bittorrent}

Add P2P applications to a blacklist.

---

### options {allow-dns | allow-icmp | allow-http | allow-ssl}

Set which basic application protocols are allowed by default. Select from the following options:

- `allow-dns`: Allow DNS traffic
- `allow-icmp`: Allow ICMP traffic
- `allow-http`: Allow generic HTTP web browsing
- `allow-ssl`: Allow generic SSL communication

The default is `allow-dns`.

---

## config entries

Configure entries on the application control list.

### risk <level>

Set the risk level for the applications. Select from the following options:

- 1: Low
- 2: Elevated
- 3: Medium
- 4: High
- 5: Critical

### category <ID>

Set the application category. Type `set category ?` to view all options.

### sub-category <ID>

Set the application sub-category. Type `set sub-category ?` to view all options. Enter `all` to include all sub-categories.

### application <ID>

Set which applications are allowed. Type `set application ?` to view all options.

### protocols <ID>

Set which protocols are allowed. Type `set protocols ?` to view all options. The default is `all`.

### vendor <ID>

Set which application vendors are allowed. Type `set vendor ?` to view all options. The default is `all`.

### technology {all | 0 | 1 | 2 | 4}

Select the technologies involved in these applications. Select from the following options:

- `all`: All technologies
- `0`: Network-Protocol
- `1`: Browser-Based
- `2`: Client-Server
- `4`: Peer-to-Peer

The default is `all`.

### behavior {all | 2 | 3 | 5 | 6 | 9}

Select the application behaviors filter. Select from the following options:

- `all`: Apply all behaviors
- `2`: Botnet
- `3`: Evasion
- `5`: Excessive bandwidth
- `6`: Tunneling
- `9`: Cloud

The default is `all`.

### popularity {1 | 2 | 3 | 4 | 5}

Enter the popularity levels of this application, with 1 being the least popular and 5 being the most popular. The default is `1 2 3 4 5`.

### tags <string>

Assign object tags.

### action {pass | block | reset}

Select the action to apply to matching traffic from the following options:

- `pass`: Allow traffic from the specified application(s)
- `block`: Stop traffic from the specified application(s)
- `reset`: Reset the network connection

The default is `block`.

### log {enable | disable}

Enable or disable logging for traffic from this list entry. The default is `enable`.

**log-packet {enable | disable}**

Enable or disable packet logging for traffic from this list entry. The default is `disable`.

**session-ttl <int>**

Set the Session TTL. The default is 0.

**quarantine {none | attacker}**

Set quarantine options for when an attack is detected. The default is `none`.

## application name

Use this command to view the application category and ID of each application. This command is read only and cannot be used to change application settings.

**config application name <application-name>**

The name of the application to view. Enter the first letter(s) of the name then use the **Tab** button to get the correct name. You can also type `?` to view all options.

**get**

Use get to view information about the application.

## application rule-settings

Configure application rule settings.

**config application rule-settings <ID>**

The ID for the rule settings entry.

**tags <tag-name>**

The tags for the rule settings entry.

## dlp

Use these commands to configure Data Leak Prevention (DLP).

This section includes descriptions for the following commands:

## dlp filepattern

Use this command to add, edit or delete the file patterns used for DLP file blocking and to set which protocols to check for files to block.

### edit <filepattern\_list\_int>

A unique integer to identify the file pattern list. `edit ?` displays existing file pattern lists and their names.  
Range: 0 - 4294967295.

### name <string>

Name of table containing the file pattern list.

### comment <string>

Enter optional comment. The comment appears in the DLP sensor list and can remind you of the details of the sensor.

## config entries

Configure file patterns used by DLP blocking.

### edit <filepattern\_str>

The name of the file pattern being configured. This can be any character string.

### filter-type {pattern | type}

Filter by file name pattern or by file type. Default is `pattern`.

- `pattern`: filter based on the file name. The pattern may include wildcards (\*). For example, blocking `*.scr` will stop all files with an `.scr` file extension.
- `type`: filter based on examination of the file contents, regardless of the file name. If you block the file type Archive (zip), all zip archives are blocked even if named with a different file extension.

### file-type <string>

This command is only available and valid when `filter-type` is set to `type`. `set file-type ?` displays all available options.

This file type filter will examine the file contents to determine the type of file and look for a match to the `file-type` specified. The file name and file extension are ignored. Because of the way the file type filter works, renaming files to make them appear to be of a different type will not allow them past the FortiGate unit without detection.

Two of the available options are not file types:

- `unknown`: to configure a rule affecting every file format the file type filter unit does not recognize. Unknown includes every file format not available in the `file-type` command.

- `ignored`: to configure a rule affecting traffic the FortiGate unit typically does not scan. This includes primarily streaming audio and video.

## dlp fp-doc-source

Use this command to add fingerprinting document sources including the server and filepath for the source files.

### edit <name\_string>

Identify the server to which DLP will be applied.

### server-type {samba}

Enter the type of DLP server. Currently only Samba (SMB) servers are supported.

### server <string>

The IPv4 or IPv6 address of the server.

### period {none | daily | weekly | monthly}

Select the frequency for server checking. Default is `none`.

### vdom {mgmt | current}

Choose whether to perform document fingerprinting from the current VDOM or the management VDOM. Files might be accessible through the management VDOM that are not accessible through the current VDOM. Default is `mgmt`.

### scan-subdirectories {enable | disable}

Enable/disable scanning of subdirectories while fingerprinting documents. Default is `enable`.

### scan-on-creation {enable | disable}

Enable/disable force scan of server when document source is created or edited. Only appears if the period is set to `daily`, `weekly`, or `monthly`. Default is `enable`.

### remove-deleted {enable | disable}

Enable/disable removing chunks of files deleted from the server. Default is `enable`.

### keep-modified {enable | disable}

Enable/disable retaining old chunks of modified files. Default is `enable`.

**username <string>**

Samba server login username.

**password <password>**

Samba server login password.

**file-path <string>**

Path to file on the server.

**file-pattern <string>**

The file pattern to match when using DLP blocking. Can include wildcards and should include file type. For example, you would enter `set file-pattern "*fortinet.xls"` to match all files that end in fortinet.xls.

**sensitivity <string>**

Sensitivity labels must be created with `config dlp fp-sensitivity` before using this command. Specify a sensitivity label to apply to source files. `set sensitivity ?` displays all available labels.

**tod-hour <integer>**

Time of day to run scans. Enter the hour only and use 24-hour clock. Only appears if the period is set to `daily`, `weekly`, or `monthly`. Default is 1.

**tod-min <integer>**

Time of day to run scans. Enter the minute only. This will only appear if the period is set to `daily`, `weekly`, or `monthly`. Default is 0.

**weekday {sunday | monday | tuesday | wednesday | thursday | friday | saturday}**

Day of the week to run scans. This will only appear if the period is set to `weekly`. Default is `sunday`.

**date <integer>**

Date of the month to run scans. This will only appear if the period is set to `monthly`. Range: 1 - 31. Default is 1.

**dlp fp-sensitivity**

Use this command to add fingerprinting sensitivity labels that can be applied to document sources and DLP rules.

## edit <name\_string>

Enter a self-explanatory string for DLP sensitivity level. It will be used when setting `sensitivity` under `config fp-doc-source`. `edit ?` displays all existing sensitivity levels.

## dlp sensor

Use this command to create a DLP sensor. The DLP sensor includes settings such as action, archive, and severity for each rule or compound rule. A number of preconfigured sensors are provided with your FortiGate. These can be edited to more closely match your needs. Consult the Handbook's discussion of [data leak prevention concepts](#) for more detail.

## comment <string>

Enter an optional description of the DLP sensor. Descriptions with spaces must be enclosed in quotes.

## replacemsg-group <group\_name>

Specify which replacement message group to use.

## dlp-log {enable | disable}

Enable/disable logging for data leak prevention. Default is `enable`.

## nac-quar-log {enable | disable}

Enable or disable logging for network access control (NAC) quarantine creation. Default is `disable`.

## flow-based {enable | disable}

Enable or disable flow-based DLP. Default is `disable`.

## full-archive-proto {smtp | pop3 | imap | http-get | http-post ftp | nntp | mapi}

Enter the protocols to always content archive.

## summary-proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}

Enter the protocols to always log summary.

## config filter

Configure DLP filters.

## edit <id\_integer>

Specify ID of filter to be configured. Range: 0-4294967295. `edit ?` displays all existing filter IDs.

**severity {info | low | medium | high | critical}**

Set the event severity. Default is `medium`.

**type {file | message}**

Select whether to check messages (for example the content of an email message) or files (for example downloaded files or the content of files attached to an email). Default is `message`.

**proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}**

Identify the protocols to detect.

**filter-by {credit-card | ssn | regexp | file-type | file-size | fingerprint | watermark | encrypted}**

Select a filter for the sensor. Default is `credit-card`.

- `credit-card`: preconfigured sensor that logs the traffic, both files and messages, that contain credit card numbers in the formats used by American Express, MasterCard and Visa.
- `ssn`: preconfigured sensor that logs the traffic containing Social Security numbers with the exception of WebEx invitation emails.
- `watermark`: Match defined file watermarks. Fortinet provides a Linux-based utility that applies a digital watermark to files. The utility adds a small (approx. 100 byte) pattern to the file that is recognized by the DLP watermark filter. The pattern is invisible to the end user. Consult the Handbook's discussion of [data leak prevention concepts](#) for more detail.
- `encrypted`: Look for encrypted files. The filter is a binary one. If the files going through the policy is encrypted, the action is triggered.

**regexp <string>**

The FortiGate checks network traffic for the regular expression specified in this regular expression filter. The regular expression library used by Fortinet is a variation of a library called PCRE (Perl Compatible Regular Expressions). Option appears when `type` is set to `file` and `filter-by` is set to `regexp`.

**file-type <integer>**

File pattern table. Option appears when `type` is set to `file` and `filter-by` is set to `file-type`. Range: 0 - 4294967295.

**file-size <integer>**

Set the file size in KB. Files over this size will match with the filter. Option appears when `type` is set to `file` and `filter-by` is set to `file-size`. Range: 0-4294967295. Default is 0.

**fp-sensitivity**

Match against a fingerprint sensitivity. Option appears when `type` is set to `file` and `filter-by` is set to `fingerprint` or `watermark`. Fingerprinting must be configured in the CLI. See also [fp-doc-source](#) and [fp-sensitivity](#). Consult the Handbook's discussion of [data leak prevention concepts](#) for more detail.



**match-percentage <integer>**

Percentage of chunks required to constitute a match. Option appears when `type` is set to `file` and `filter-by` is set to `fingerprint`. Range: 0-100. Default is 0.

**company-identifier**

Company identifier for watermarking. Option appears when `type` is set to `file` and `filter-by` is set to `watermark`. Ensures that you are only blocking watermarks that your company has placed on the files, not watermarks with the same name but place by other companies.

**action {allow | log-only | block | quarantine-ip}**

Specify action to take when a match is detected. Default is `allow`.

- `allow`: no action is taken even if the patterns specified in the filter are matched.
- `log-only`: the FortiGate will take no action on network traffic matching a rule with this action. The filter match is logged
- `block`: traffic matching a filter with the block action will not be delivered.
- `quarantine-ip`: block access through the FortiGate unit for any IP address that sends traffic matching a sensor with this action. The IP address is added to the Banned User list for a duration of time that is determined by `set expiry`.

**expiry <###d##h##m>**

Set the duration of the quarantine in the days, hours, minutes format `dddhhmm ###d##h##m`. Only appears if `action` is set to `quarantine-ip`. Range: 0d0h1m -364d23h59m. Default is 5m.

## dlp settings

Use this command to designate logical storage settings for the DLP fingerprinting database.

**storage device <string>**

Enter the storage device name.

**size <integer>**

Enter the maximum total size of files in storage in MB. Default is 16.

**db-mode {remove-modified-then-oldest | remove-oldest | stop-adding}**

Select the method of maintaining the database size. Default is `stop-adding`.

- `remove-modified-then-oldest`: remove oldest chunks first, and then remove oldest file entries.
- `remove-oldest`: just remove the oldest files first.
- `stop-adding`: don't remove files, just stop adding to database.

### cache-mem-percent <integer>

Enter the maximum percentage of available memory allocated to caching. Range: 1 - 15 %. Default is 2.

### chunk-size <integer>

Maximum fingerprint chunk size.

Changing the chunk size will flush the entire database. Document source fingerprints will repopulate with the next scan. Only manually updated fingerprints will be lost. Range: 100 - 100000. Default is 2800. Smaller chunks allow for greater precision, but at the cost of increased processing, database size, and lookups.

## endpoint-control

Use endpoint-control commands to configure the following parts of the Endpoint NAC feature:

- Endpoint license registration synchronization
- Endpoint NAC profiles
- the required minimum version of FortiClient Endpoint Security
- the FortiClient installer download location

Endpoint NAC is enabled in firewall policies.

## endpoint-control forticlient-registration-sync

## endpoint-control profile

## endpoint-control settings

## firewall

Use firewall commands to configure firewall policies and the data they use.

## firewall address | address6

Use this command to configure firewall addresses used in firewall policies. An IPv4 firewall address is a set of one or more IP addresses, represented as a domain name, an IP address and a subnet mask, or an IP address range. An IPv6 firewall address is an IPv6 address prefix. Addresses, address groups, and virtual IPs must have unique

names to avoid confusion in firewall policies. If an address is selected in a policy, it cannot be deleted until it is deselected from the policy.

### Syntax

```
config firewall {address | address6}
    {edit|delete|rename|get|show} <name_str>
```

## Managing address objects

The configuration of specific address object is the most common activity when using the config firewall address command but some commands affect the address objects as a whole.

### edit

Used to select which individual address object to configure or edit values.

```
edit <address_name>
```

To get a list of all of the existing address objects, type the command:

```
Command Prompt (address) # edit ?
or
Command Prompt (address6) # edit ?
```

If you are creating a new address object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

### delete

Used to delete an existing address object

```
delete <address_name>
```

- The <address\_name> can be a string of up to 64 characters.

### purge

Used to delete all of the existing address or address6 objects. It deletes all of the values within the table that holds the information about address or address6 objects within the VDOM.

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

### rename

Used to change the name of the address object.

```
rename <address_name> to <new_address_name>
```

---

### name

This field is a unique name given to represent the address object. This setting is for both IPv4 and IPv6. This setting is first defined when using the edit command to edit an address object that does not currently exist. This

setting is available for both `address` and `address6`. The name field of an address object cannot be changed from within the object. It can be changed by using the `rename` command in the `config firewall address` or `config firewall address6` context.

## uuid

Each address has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited. This setting is available for both `address` and `address6`.

### Syntax:

```
set uuid <uuid>
```

**Default value:** autogenerated

### Example:

```
config firewall address
    edit example.com
        set uuid d38e0dca-b80c-51e6-1180-6863e1b9ea9a
    end
```

## subnet

The IP address and subnet mask of the address. By using different subnet masks a single IP address can be defined or a group of addresses. This setting is only available for `address`. This option is available only if the `type` option is set to `ipmask`.

### Syntax:

```
set subnet <ipv4-classnet-any>
```

**Default value:** 0.0.0.0 0.0.0.0

### Example:

```
config firewall address
    edit example.com
        set type ipmask
        set subnet 192.168.1.1 255.255.255.255
    or ...
        set subnet 192.168.1.1/32
    end
```

## type

This field sets the type of address object. There are two sets of types for addresses. The first is for IPv4 addresses the second is for IPv6.

IPv4 types

- `ipmask` - a standard IPv4 address with subnet mask
- `iprange` - a range of IPv4 addresses between two specified addresses (inclusive).
- `fqdn` - a Fully Qualified Domain Name address
- `geography` - IP addresses from a specified country
- `wildcard` - a standard IPv4 using a wildcard subnet mask
- `wildcard-fqdn` - a Fully Qualified Domain Name with wildcard characters

#### IPv6 types

- `ipprefix` - uses the IP prefix to define a range of IPv6 addresses
- `iprange` - a range of IPv6 addresses between two specified addresses (inclusive).

#### Syntax:

```
set type {ipmask | iprange | fqdn | geography | wildcard | wildcard-fqdn}
```

**Default value:** `ipmask` or

```
set type {ipprefix | iprange}
```

**Default value:** `ipprefix`

#### Example:

```
config firewall address
    edit example.com
        set type ipmask
    end
```

## ip6

This is for the IPv6 address prefix. This setting is only available for `address6`.

#### Syntax:

```
set ip6 <ipv6-network>
```

**Default value:** `::/0`

#### Example:

```
config firewall address6
    edit example.com
        set ip6 2001:db8:a0b:12f0::1/64
    end
```

## start-ip

The first IP address (inclusive) in the range for the address. This setting is available for both `address` and `address6`. This option is available only if the `type` option is set to `iprange`.

**Syntax:**

```
set start-ip <ipv4-address-any>
```

**Default value:** 0.0.0.0 0.0.0.0 or

```
set start-ip <ipv6-address>
```

**Default value:** ::

**Example:**

```
config firewall address
  edit example.com
  set type iprange
  set start-ip 192.168.1.43
or ...
config firewall address6
  edit example.com
  set type iprange
  set start-ip 2001:db8:a0b:12f0::1
```

## end-ip

The final IP address (inclusive) in the range for the address. This setting is available for both `address` and `address6`. This option is available only if the `type` option is set to `iprange`.

**Syntax:**

```
set end-ip <ipv4-address-any>
```

**Default value:** 0.0.0.0 0.0.0.0 or

```
set end-ip <ipv6-address>
```

**Default value:** ::

**Example:**

```
config firewall address
  edit example.com
  set type iprange
  set end-ip 192.168.1.201
or ...
config firewall address6
  edit example.com
  set type iprange
  set end-ip 2001:db8:a0b:12f0::89
```

## fqdn

This setting defines a Fully qualified domain name which is normally translated to an IP address by a DNS server. This setting is only available for `address`. This option is available only if the `type` option is set to `fqdn`.

**Syntax:**

```
set fqdn <string>
```

**Example:**

```
config firewall address
  edit example.com
    set type fqdn
    set fqdn example.com
end
```

## country

This field is used to set the country and all of its IP addresses. This setting is only available for `address`. This option is available only if the `type` option is set to `geography`. The options in this field are 2 character country code that represent different countries or other options. To get a listing type the command `set country ?`. An example of some of the available options are:

ZZ	Reserved
A1	Anonymous Proxy
A2	Satellite Provider
O1	Other Country
AD	Andorra
.	
.	
.	
ZW	Zimbabwe

**Syntax:**

```
set country <2 character string>
```

**Example:**

```
config firewall address
  edit example.com
    set type geography
    set country US
end
```

## wildcard-fqdn

A Fully Qualified Domain Name, but using wildcard symbols in place of some of the characters. This setting is only available for `address`. This option is available only if the `type` option is set to `wildcard-fqdn`.

**Syntax:**

```
set wildcard-fqdn <string>
```

**Example:**

```
config firewall address
    edit example.com
        set wildcard-fqdn *.example.com
    end
```

## cache-ttl

This setting defines the minimal TTL (time to live) of individual IP addresses in FQDN cache. The TTL is measured in seconds. This setting is only available for `address`. This option is available only if the `type` option is set to `fqdn`.

**Syntax:**

```
set cache-ttl <integer>
```

**Default value:** 0 **Example:**

```
config firewall address
    edit example.com
        set cache-ttl 3600
```

## wildcard

This setting defines an IP address and a wildcard netmask. This setting is only available for `address`. This option is available only if the `type` option is set to `wildcard`.

**Syntax:**

```
set wildcard <ipv4-classnet-any>
```

**Default value:** 0.0.0.0 0.0.0.0

**Example:**

```
config firewall address
    edit example.com
        set wildcard 192.168.0.0 255.255.0.64
    end
```

## comment

Field used to store descriptive information about the address. The field is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces. This setting is available for both `address` and `address6`.

**Syntax:**

```
set comment <var-string>
```



**Example:**

```
config firewall address
    edit example.com
        set comment "Address for the Example Company website"
    end
```

## visibility

Enables or disables the ability to see the address in the GUI. This setting is available for both `address` and `address6`.

**Syntax:**

```
set visibility {enable | disable}
```

**Default value:** enable

**Example:**

```
config firewall address
    edit example.com
        set visibility disable
    end
```

## associated-interface

Use this option to associate the address to a specific interface on the FortiGate. The address will only be available for selection if the associated interface is associated to the policy. The option to choose any interface is also available. This setting is only available for `address`.

**Syntax:**

```
set associated-interface <string>
```

**Example:**

```
config firewall address
    edit example.com
        set associated-interface wan1
    end
```

## color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1. This setting is available for both `address` and `address6`.

**Syntax:**

```
set color <integer>
```

**Default value:** 0

**Example:**

```
config firewall address
    edit example.com
        set color 15
    end
```

## tags

Used to assign a custom tag to the address object. The tags need to be preconfigured in `config system object-tag` and the same list of tags can be used anywhere that the tag setting is available. To see what tags are available for use, use the command `set tags ?`. This setting is available for both `address` and `address6`. Separate multiple values with a space.

**Syntax:**

```
{set|append|clear} tags <name_of_tag>
```

**Example:**

```
config system object-tag
    edit example-tag1
    next
    edit example-tag2
    next
    edit "example tag 3"
    next
end

config firewall address
    edit example.com
        set tags example-tag1 example-tag2
        append "example tag 3"
    end
```

## allow-routing

Enable/disable use of this address in the static route configuration. This setting is only available for `address`.

**Syntax:**

```
set allow-routing {enable | disable}
```

**Default value:** disable

**Example:**

```
config firewall address
    edit example.com
```

```
        set allow-routing enable
    end
```

## firewall addrgrp | addgrp6

Use this command to configure firewall address groups used in firewall policies. You can organize related firewall addresses into firewall address groups to simplify firewall policy configuration. For example, rather than creating three separate firewall policies for three firewall addresses, you could create a firewall address group consisting of the three firewall addresses, then create one firewall policy using that firewall address group. Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies. If an address group is selected in a policy, it cannot be deleted unless it is first deselected in the policy. An address group can be a member of another address group.

### Syntax

```
config firewall {addrgrp | addgrp6}
    {edit|delete|purge|rename|get|show} <name_str>
```

## Managing address objects

The configuration of specific address object is the most common activity when using the config firewall address command but some commands affect the address objects as a whole.

### edit

Used to select which individual policy to configure or edit values.

```
edit <address_group>
```

To get a list of all of the existing address objects, type the command:

```
Command Prompt (addrgrp) # edit ?
or
Command Prompt (addgrp6) # edit ?
```

If you are creating a new address object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

### delete

Used to delete an existing address object

```
delete <address_group>
```

- The <address\_group> can be a string of up to 64 characters.

### purge

Used delete all of the existing addrgrp or addgrp6 objects. It deletes all of the values within the table that holds the information about addrgrp or addgrp6 objects within the VDOM.

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

## rename

Used to change the name of the addrgrp or addrgrp6 object.

```
rename <address_group> to <new_address_group>
```

---

## name

This field is a unique name given to represent the address group object. This settings is for both IPv4 and IPv6. This setting is first defined when using the edit command to edit an address group object that does not currently exist. The name field of an address object cannot be changed from within the object. It can be changed by using the rename command in the `config firewall addrgrp` or `config firewall addrgrp6` context.

## uuid

Each address has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited. This settings is for both IPv4 and IPv6.

### Syntax:

```
set uuid <uuid>
```

**Default value:** autogenerated

### Example:

```
config firewall addrgrp
edit example_group
set uuid d38e0dca-b80c-51e6-1180-6863e1b9ea9a
end
```

## member

Defines the address objects that are members of the address group. The value is a <string> that should be the name of one of the existing address objects configured on the device. A group cannot contain both IPv4 and IPv6 address objects. Separate multiple interfaces with a space.

### Syntax:

```
{set|append} members <name of address object> [<name of address object> ...]
```

### Example:

```
config firewall addrgrp
edit example_group
set member example_address1
or ...
set member example_address1 example_address2
```

```
    or ...
    append example_address3
end
```

## comment

Field used to store descriptive information about the address group. The field is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces. This settings is for both IPv4 and IPv6.

### Syntax:

```
set comment <var-string>
```

### Example:

```
config firewall addrgrp
    edit example.com
        set comment "Addresses for Vendor Websites"
    end
```

## visibility

Enables or disables the ability to see the address group in the GUI. This settings is for both IPv4 and IPv6.

### Syntax:

```
set visibility {enable | disable}
```

**Default value:** enable

### Example:

```
config firewall addrgrp
    edit example_group
        set visibility disable
    end
```

## color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1. This settings is for both IPv4 and IPv6.

### Syntax:

```
set color <integer>
```

**Default value:** 0

### Example:

```
config firewall addrgrp
    edit example_group
```

```
        set color 7
    end
```

## tags

Used to assign a custom tag to the address group object. The tags need to be preconfigured in `config system object-tag` and the same list of tags can be used anywhere that the tag setting is available. To see what tags are available for use, use the command `set tags ?`. This settings is for both IPv4 and IPv6. Separate multiple values with a space.

### Syntax:

```
{set|append|clear} tags <name_of_tag>
```

### Example:

```
config system object-tag
    edit example-tag1
    next
    edit example-tag2
    next
    edit "example tag 3"
    next
end

config firewall addrgrp
    edit example_group
    set tags example-tag1 example-tag2
    append "example tag 3"
end
```

## allow-routing

Enable/disable use of this address group in the static route configuration. This option is only available for IPv4.

### Syntax:

```
set allow-routing {enable | disable}
```

**Default value:** disable

### Example:

```
config firewall addrgrp
    edit example_group
    set allow-routing enable
end
```

## firewall policy | policy6

Used to change firewall policies or their individual configurations. In addition to editing an existing policy, policies can be added, deleted, moved or cloned. It is also possible to purge all of the policy content from the table that holds them.

- Use `config firewall policy` for IPv4 policies
- Use `config firewall policy6` for IPv6 policies

Firewall policies control all traffic passing through the FortiGate unit. Firewall policies are instructions used by the FortiGate unit to decide what to do with a connection request. The policy directs the firewall to allow the connection, deny the connection, require authentication before the connection is allowed, or apply IPSec processing. The commands `config firewall policy` and `config firewall policy6` enter the system into the correct context of the configuration file to make changes to firewall policies. From here, a specific policy is chosen to be acted upon.

### Managing policy objects

The configuration of specific policy options or settings is the most common activity when using the firewall policy command but some commands affect the policy objects as a whole.

#### edit

Used to select which individual policy to configure or edit values.

##### Syntax:

```
edit <policyid>
```

- Choosing 0 as the `<policyid>` will add a new policy using the next available number as the `<policyid>`. While first editing the policy the context at the command prompt will indicate that the `<policyid>` is 0 but subsequent editing will require going to the new `<policyid>`.

#### delete

Used to delete an existing firewall policy

##### Syntax:

```
delete <policyid>
```

- The `<policyid>` can be an integer value between 0 and 4294967294

#### purge

Used delete all of the existing firewall policies. It deletes all of the values within the table that holds the information about firewall policies within the VDOM.

##### Syntax:

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

### move

Used to move the position of a policy, relative to another policy, in the sequence order of how policies are applied.

#### Syntax:

```
move <policyid> {after | before} <policyid>
```

### clone

Used to copy all of the attributes of an existing policy to another policy.

#### Syntax:

```
clone <policyid> to <policyid>
```

## Options and settings within a policy

### name

A unique name given to the policy. By default, this is a required field but the requirement can be disabled.

#### Syntax:

```
set name <string>
```

#### Examples:

```
config firewall policy
    edit 0
        set name example
    or..
        set name "example policy name"
end
```

### uuid

Each policy has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited.

#### Syntax:

```
set uuid <uuid_value>
```

**Default value:** autogenerated



**Example:**

```
config firewall policy
    edit 0
        set uuid a3c9ccb8-a84a-51e6-d72c-6a5189cadb83
    end
```

**srcintf**

Sets the source interface of the traffic that the policy will manage. The value is a <string> that should be the name of one of the existing interfaces configured on the device. Separate multiple interfaces with a space.

**Syntax:**

```
{set|append} srcintf <name_of_interface> [<name_of_interface> ...]
```

**Example:**

```
config firewall policy
    edit 0
        set srcintf port1
    or ...
        set srcintf port2 port3
    or ...
        append srcintf port4
    end
```

**dstintf**

Sets the destination interface of the traffic that the policy will manage. The value is a <string> that should be the name of one of the existing interfaces configured on the device. Separate multiple interfaces with a space.

**Syntax:**

```
{set|append} dstintf <name_of_interface> [<name_of_interface> ...]
```

**Example:**

```
config firewall policy
    edit 0
        set dstintf port11
    or ...
        set dstintf port12 port13
    or ...
        append distintf port14
    end
```

**srcaddr**

Sets the source address object(s), whose traffic will be managed by this policy. More than once object can be assigned to this option. Separate multiple addresses with a space.

**Syntax:**

```
{set|append} srcaddr <address_object> [<address_object> ...]
```

**Examples:**

```
config firewall policy
  edit 0
  set srcaddr example_address1
  or ...
  set srcaddress "example address2" "example_address3"
  or ...
  append srcaddr example_address4
end
```

**dstaddr**

Sets the destination address object(s), whose traffic will be managed by this policy. More than once object can be assigned to this option. Separate multiple addresses with a space.

**Syntax:**

```
{set|append} dstaddr <address_object> [<address_object> ...]
```

**Examples:**

```
config firewall policy
  edit 0
  set dstaddr example_address1
  or ...
  set dstaddr "example address2" "example_address3"
  or ...
  append dstaddr example_address4
end
```

**rtp-nat**

Enables or disables the application of source NAT to RTP packets received by the firewall policy. This field is used for redundant SIP configurations. If `rtp-nat` is enabled you must add one or more firewall addresses to the `rtp-addr` field.

**Syntax:**

```
set rtp-nat {enable|disable}
```

**Default value:** disable

**rtp-addr**

Used to enter one or more RTP firewall addresses for the policy. This field is only available when `rtp-nat` is enabled. Separate multiple addresses with a space.

**Syntax:**

```
{set|append} rtp-addr <address_object> [<address_object> ...]
```

**Examples:**

```
config firewall policy
    edit 0
    set rtp-addr example_address1
    or ...
    set rtp-addr "example address 2" "example_address3
    or ...
    append example_address4
end
```

**learning-mode**

Enables or disables a specialized action option that monitors and logs traffic based on hard coded security profiles. See [Make it a policy to learn before configuring policies](#). Enabling `learning-mode` will make the `action` setting unavailable.

**Syntax:**

```
set learning-mode {enable|disable}
```

**Default value:** `disable`

**action**

Sets the action that the FortiGate unit will perform on traffic matching this firewall policy.

- `accept` — Allow packets that match the firewall policy. Optionally, also enable `nat` to make this a NAT policy (NAT/Route mode only).
- `deny` — Deny packets that match the firewall policy.
- `ipsec` — Allow and apply IPSec VPN. You must specify the `vpntunnel` attribute. You may also enable or disable the `inbound`, `outbound`, `natoutbound`, and `natinbound` attributes and/or specify a `natip` value.

**Limitations:**

- If `learning-mode` is enabled the `action` setting will not be available
- For IPv6 policies, only `accept` and `deny` options are available.

**Syntax:**

```
set action [accept|deny|ipsec]
```

**Default value:** `deny`

**Examples:**

```
config firewall policy
    edit 0
    set action accept
end
```

**send-deny-packet**

Enables or disables the ability to send a packet in reply to denied TCP, UDP or ICMP traffic. When `deny-tcp-with-icmp` is enabled in system settings, a Communication Prohibited ICMP packet is sent. Otherwise,

denied TCP traffic is sent a TCP reset.

**Syntax:**

```
set send-deny-packet {enable|disable}
```

**Default value:** disable

**firewall-session-dirty**

Used to determine whether changes to a firewall policy affect all sessions or just new ones.

- `check-all` — flushes all current sessions in order to re-evaluate them
- `check-new` — keeps existing sessions and applies policy change only to new sessions

This field is available if `firewall-session-dirty` in `config system settings` is set to `check-policy-option`.

**Syntax:**

```
set firewall-session-dirty [check-all|check-new]
```

**Default value:** check-all

**Examples:**

```
config firewall policy
    edit 0
        set firewall-session-dirty check-new
    end
```

**status**

Enables or disables a policy.

**Syntax:**

```
set status {enable|disable}
```

**Default value:** enable

**schedule**

Sets the schedule used by the policy. The variable is the name of the existing one-time or reoccurring schedule, or schedule group.

**Syntax:**

```
set schedule <schedule_object>
```

**Examples:**

```
config firewall policy
    edit 0
```

```
        set schedule work_week
    end
```

### schedule-timeout

When enabled, sessions are forced to end when the schedule's end time is reached. If disabled, sessions can go past the schedule's end time, but no new sessions can start.

#### Syntax:

```
set schedule-timeout {enable|disable}
```

**Default value:** disable

### service

Used to set the services matched by the policy. The variable can be one or more services or service groups. Separate multiple services with a space.

#### Syntax:

```
{set|append} service <service_object> [<service_object> ...]
```

#### Examples:

```
config firewall policy
    edit 0
    set service http
    or ...
    set service http "Email Access"
    or ...
    append service ftp
end
```

### utm-status

Enables or disables adding security profiles on the firewall policy. If enabled, at least one profile must be added to the policy. This setting is not available until the source and destination parameters of the policy have been configured.

#### Syntax:

```
set utm-status {enable|disable}
```

**Default value:** disable

### profile-type

Sets whether or not to use individual UTM profiles or a UTM profile group to the firewall policy.

#### Syntax:

```
set profile-type {single | group}
```

**Default value:** single

**Examples:**

```
config firewall policy
    edit 0
        set profile-type group
    end
```

**profile-group**

Determines the name of a UTM profile group in the firewall policy. This option is available if `profile-type` is set to `group`.

**Syntax:**

```
set profile-group <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set profile-group example_profile_group
    end
```

**av-profile**

Sets the name of the antivirus profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

**Syntax:**

```
set av-profile <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set av-profile default_av_profile
    end
```

**webfilter-profile**

Sets the name of the webfilter profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

**Syntax:**

```
set webfilter-profile <string>
```

**Example:**

```
config firewall policy
    edit 0
```

```
        set webfilter-profile "example web profile"
    end
```

### dnsfilter-profile

Sets the name of the DNS filter profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

#### Syntax:

```
set dnsfilter-profile <string>
```

#### Examples:

```
config firewall policy
    edit 0
        set dnsfilter-profile dns_for_developers
    end
```

### spamfilter-profile

Sets the name of the spam filter profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

#### Syntax:

```
set spamfilter-profile <string>
```

#### Examples:

```
config firewall policy
    edit 0
        set spamfilter-profile spam-filter1
    end
```

### dlp-sensor

Sets the name of the DLP sensor profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

#### Syntax:

```
set dlp-sensor <string>
```

#### Examples:

```
config firewall policy
    edit 0
        set dlp-sensor dlp-classified
    end
```

## ips-sensor

Sets the name of the IPS profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

### Syntax:

```
set ips-sensor <string>
```

### Examples:

```
config firewall policy
    edit 0
        set ips-sensor production_ips
    end
```

## application-list

Sets the name of the pre-packaged list of applications associated with the firewall policy. This field is available only if `utm-status` is enabled.

### Syntax:

```
set application-list <string>
```

### Examples:

```
config firewall policy
    edit 0
        set application-list allowed-apps
    end
```

## casi-profile

Sets the name of the CASI profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

### Syntax:

```
set casi-profile <string>
```

### Examples:

```
config firewall policy
    edit 0
        set casi-profile casi-default
    end
```

## voip-profile

Sets the name of the VoIP profile associated with the firewall policy. This field is available only if `utm-status` is enabled.



**Syntax:**

```
set voip-profile <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set voip-profile voip-example
    end
```

**icap-profile**

Sets the name of the ICAP profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

**Syntax:**

```
set icap-profile <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set icap-profile icap-test
    end
```

**waf-profile**

Sets the name of the WAF profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

**Syntax:**

```
set waf-profile <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set waf-profile waf-profile1
    end
```

**profile-protocol-options**

Sets the name of the protocol options profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

**Syntax:**

```
set profile-protocol-options <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set profile-protocol-options company_default
    end
```

**ssl-ssh-profile**

Sets the name of the SSL/SSH profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

**Syntax:**

```
set ssl-ssh-profile <string>
```

**Examples:**

```
config firewall policy
    edit 0
        set ssl-ssh-profile default-profile
    end
```

**logtraffic**

Used to set how traffic logs are recorded for this policy.

- `all` - record logs for all traffic accepted by this policy
- `utm` log traffic traffic that has a security profile applied to it
- `disable` - disable logging for this policy

**Syntax:**

```
set logtraffic {all | utm | disable}
```

**Default value:** `utm`

**Example:**

```
config firewall policy
    edit 0
        set logtraffic utm
    end
```

**logtraffic-start**

Enables or disables the ability to log session starts and stops.

**Syntax:**

```
set logtraffic-start {enable|disable}
```

**Default value:** `disable`

### capture-packet

Enables or disables the packet capture feature. This is available if the `logtraffic` setting is `all` or `utm`.

**Default value:** `disable`

**Syntax:**

```
set capture-packet {enable|disable}
```

### auto-asic-offload

Enables or disables offloading policy traffic to CP processors.

**Syntax:**

```
set auto-asic-offload {enable|disable}
```

**Default value:** `disable`

### wanopt

Enables or disables the use the the WAN optimization feature on this policy. This feature is only available if the `action` setting is `accept`.

**Syntax:**

```
set wanopt {enable|disable}
```

**Default value:** `disable`

### wanopt-detection

Used to select the wanopt peer auto-detection mode.

**Syntax:**

```
set wanopt-detection {active | passive | off}
```

**Default value:** `off`

**Example:**

```
config firewall policy
    edit 0
        set wanopt-detection active
    end
```

### wanopt-passive-opt

Used to set passive WAN Optimization policy address translation behavior.

- `default` - Use the transparent setting in the WAN Optimization profile added to the active policy (client-side configuration).

- **transparent** - Impose transparent mode (override the active policy transparent mode setting). Packets exiting the FortiGate keep their original source addresses.
- **non-transparent** - Impose non-transparent mode (override the active policy transparent mode setting). Packets exiting the FortiGate have their source address changed to the address of the server-side FortiGate unit interface that sends the packets to the servers.

**Syntax:**

```
set wanopt-passive-opt {default | transparent | non-transparent}
```

**Default value:** default

**Example:**

```
config firewall policy
    edit 0
        set wanopt-passive-opt transparent
    end
```

**wanopt-profile**

Sets the name of the WAN optimization profile associated with the firewall policy.

**Syntax:**

```
set wanopt-profile <string>
```

**Example:**

```
config firewall policy
    edit 0
        set wanopt-profile "Company default WANopt"
    end
```

**wanopt-peer**

Used to set the WAN optimization peer.

**Syntax:**

```
set wanopt-peer <string>
```

**webcache**

Enables or disables the WAN optimization web caching for HTTP traffic accepted by the firewall policy. This option is available only on FortiGate units that support WAN Optimization and web caching.

**Syntax:**

```
set webcache {enable|disable}
```

**Default value:** disable

## webcache-https

Sets the level of webcaching for HTTPS traffic.

- `disable` — no caching of HTTPS traffic
- `enable` — caching of HTTPS traffic

This field is available only if `webcache` is enabled. This field is not available if `srcintf` is `ftp-proxy` or `wanopt`.

### Syntax:

```
set webcache-https {disable| enable}
```

**Default value:** `disable`

### Example:

```
config firewall policy
    edit 0
        set webcache enable
        set webcache-https enable
    end
```

## traffic-shaper

Select a traffic shaper for the policy. A traffic shaper controls the bandwidth available to, and sets the priority of the traffic processed by, the policy.

### Syntax:

```
set traffic-shaper <string>
```

## traffic-shaper-reverse

Select a reverse traffic shaper. For example, if the traffic direction that a policy controls is from port1 to port2, select this option will also apply the policy shaping configuration to traffic from port2 to port1.

### Syntax:

```
set traffic-shaper-reverse <string>
```

## per-ip-shaper

Enter the name of the per-IP traffic shaper to associate with this policy. For information about per-IP traffic shapers, see `firewall shaper per-ip-shaper`.

### Syntax:

```
set per-ip-shaper <string>
```

## nat

Enables or disables the use of Network Address Translation (NAT)

**Syntax:**

```
set nat {enable|disable}
```

**Default value:** disable

**permit-any-host**

Enables or disables the ability to accept UDP packets from any host. This can help support the FaceTime application on NAT'd iPhones.

**Syntax:**

```
set permit-any-host {enable|disable}
```

**Default value:** disable

**permit-stun-host**

Enables or disables the ability to accept UDP packets from any Session Traversal Utilities for NAT (STUN) host. This can help support the FaceTime application on NAT'd iPhones.

**Syntax:**

```
set permit-stun-host {enable|disable}
```

**Default value:** disable

**fixedport**

Enables or disables the ability to preserve packets' source port number, which may otherwise be changed by a NAT policy. Some applications do not function correctly if the source port number is changed, and may require this option. If `fixedport` is `enable`, you should usually also enable IP pools; if you do not configure an IP pool for the policy, only one connection can occur at a time for this port.

**Syntax:**

```
set fixedport {enable|disable}
```

**Default value:** disable

**ippool**

Enables or disables the use of ippools for NAT. When the `action` is set to `accept` and NAT is enabled, the `ippool` function allows a NAT policy to translate the source address to an address randomly selected from the first IP pool added to the destination interface of the policy.

**Syntax:**

```
set ippool {enable|disable}
```

**Default value:** disable

## poolname

The name of the IP pool to be used for NAT. To use this option requires that `ippool` be enabled. Separate multiple addresses with a space.

### Syntax:

```
{set|append} poolname <ippool> [<ippool> ...]
```

### Example:

```
config firewall policy
    edit 0
    set poolname testpool1
    or ...
    append poolname "testpool 1" "testpool2"
    or ...
    clear poolname
end
```

## session-ttl

Used to set the timeout value in the policy to override the global timeout setting defined by using `config system session-ttl`. When it is on default value, it will not take effect. Value is in seconds.

### Syntax:

```
set session-ttl <integer>
```

**Default value:** 0

### Example:

```
config firewall policy
    edit 0
    set session-ttl 3600
end
```

## vlan-cos-fwd

Used to set the VLAN forward direction user priority, CoS. Range 0 (lowest) to 7 (highest), 255 for passthrough.

### Syntax:

```
set vlan-cos-fwd <integer>
```

**Default value:** 255

### Example:

```
config firewall policy
    edit 0
    set vlan-cos-fwd 7
end
```

## vlan-cos-rev

Used to set the VLAN reverse direction user priority, CoS. Range 0 (lowest) to 7 (highest), 255 for passthrough.

### Syntax:

```
set vlan-cos-rev <integer>
```

**Default value:** 255

### Example:

```
config firewall policy
    edit 0
        set vlan-cos-rev 3
    end
```

## inbound

When `action` is set to `ipsec`, this setting enables or disables traffic from computers on the remote private network to initiate an IPSec VPN tunnel.

### Syntax:

```
set inbound {enable | disable}
```

**Default value:** disable

## outbound

When `action` is set to `ipsec`, this setting enables or disables traffic from computers on the local private network to initiate an IPSec VPN tunnel.

### Syntax:

```
set outbound {enable | disable}
```

**Default value:** disable

## natinbound

Enables or disables the function of translating the source addresses IP packets emerging from an IPsec tunnel into the IP address of the FortiGate unit's network interface to the local private network. This option appears only if `action` is `ipsec`.

### Syntax:

```
set natinbound {enable | disable}
```

**Default value:** disable

## natoutbound

Enables or disables the function of translating the source addresses of outbound encrypted packets into the IP address of the FortiGate unit's outbound interface. Enable this attribute in combination with the `natip` attribute



to change the source addresses of IP packets before they go into the tunnel. This option appears only if attribute to change the source addresses of IP packets before they go into the tunnel. This option appears only if `action` is `ipsec`.

**Syntax:**

```
set natoutbound {enable | disable}
```

**Default value:** `disable`

**wccp**

Enables or disables Web Cache Coordination Protocol (WCCP). If enabled, the traffic accepted by this policy is sent to a configured WCCP server as configured by the `config system wccp` command.

**Syntax:**

```
set wccp {enable|disable}
```

**Default value:** `disable`

**ntlm**

Enables or disables Directory Service authentication via NTLM. If you enable this option, you must also define the user groups. This field is available only if the `groups` or `users` fields are specified.

**Syntax:**

```
set ntlm {enable|disable}
```

**Default value:** `disable`

**ntlm-guest**

Enables or disables NTLM guest user access.

**Syntax:**

```
set ntlm-guest {enable|disable}
```

**Default value:** `disable`

**ntlm-enabled-browsers**

Sets the value for the HTTP-User-Agent of supported browsers. Enclose each string in quotes and separate strings with a space. Browsers with non-matching strings get guest access.

**Syntax:**

```
{set|append|clear} ntlm-enabled-browsers <user_agent_string>
```

**fssso**

Enables or disables Fortinet Single Sign On. This field is available when `groups` is populated.

**Syntax:**

```
set fsso {enable|disable}
```

**Default value:** disable

**WSSO**

Enables or disables WiFi Single Sign On.

**Syntax:**

```
set wssso {enable|disable}
```

**Default value:** disable

**rssso**

Enables or disables RADIUS-based single sign-on (SSO) for this policy.

**Syntax:**

```
set rssso {enable|disable}
```

**Default value:** disable

**fsso-agent-for-ntlm**

Specify FSSO agent for NTLM authentication.

**Syntax:**

```
set fsso-agent-for-ntlm <string>
```

**groups**

A listing of the names of the user groups allowed to use this policy. Separate multiple groups with a space.

**Syntax:**

```
{set|append} groups <user-group_object> [<user-group_object> ...]
```

**Examples:**

```
config firewall policy
  edit 0
    set groups group1
  or ...
  set groups group2 "Group 3"
  or ...
  append groups group4
end
```

**users**

A listing of the names of the users allowed to use this policy. Separate multiple users with a space.

**Syntax:**

```
{set|append} users <user_object> [<user_object> ...]
```

**Examples:**

```
config firewall policy
  edit 0
    set users adam
  or ...
  set users burt "Charlie C"
  or ...
  append users david
end
```

**devices**

A listing of the names of devices or device categories that apply to this policy. Separate multiple devices with a space.

**Syntax:**

```
{set|append} devices <device_object> [<device_object> ...]
```

**Examples:**

```
config firewall policy
  edit 0
    set devices "adams pc"
  or ...
  set user bob-pc linux-pc
  or ...
  append user windows-pc
end
```

**auth-path**

Enables or disables authentication-based routing. You must also specify a RADIUS server, and the RADIUS server must be configured to supply the name of an object specified in `config router auth-path`. For details on configuring authentication-based routes, see `router auth-path`. This field is available only when the FortiGate unit is operating in NAT mode and the `groups` or `users` fields are specified.

**Syntax:**

```
set auth-path {enable|disable}
```

**Default value:** disable

**disclaimer**

Enables or disables the display of the authentication disclaimer page, which is configured with other replacement messages. The user must accept the disclaimer to connect to the destination.

**Syntax:**

```
set disclaimer {enable|disable}
```

**Default value:** disable

**vpntunnel**

Sets the name of a Phase 1 IPsec VPN configuration to apply to the IPsec tunnel. This field is available only if `action` is `ipsec`.

**Syntax:**

```
set vpntunnel <string>
```

**Example:**

```
config firewall policy
    edit 0
        set vpntunnel "TunnelA Phase 1"
    end
```

**natip**

Used to specify the source IP address and subnet mask to apply to outbound clear text packets before they are sent through the tunnel. If you do not specify a `natip` value when `natoutbound` is enabled, the source addresses of outbound encrypted packets are translated into the IP address of the FortiGate unit's external interface. When a `natip` value is specified, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate the source addresses of outbound IP packets into corresponding IP addresses on the subnetwork that you specify. For example, if the source address in the firewall encryption policy is 192.168.1.0/24 and the `natip` value is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7. This field is available only if `ipsec` and `natoutbound` is enabled.

**Syntax:**

```
set natip <IP_address> <IPv4mask>
```

**match-vip**

Enables or disables the function of matching DNATed packets. If you want to explicitly drop a packet that is not matched with a firewall policy and write a log message when this happens, you can add a general policy (source and destination address set to ANY) to the bottom of a policy list and configure the firewall policy to DENY packets and record a log message when a packet is dropped. In some cases, when a virtual IP performs destination NAT (DNAT) on a packet, the translated packet may not be accepted by a firewall policy. If this happens, the packet is silently dropped and therefore not matched with the general policy at the bottom of the policy list. To catch these packets, enable `match-vip` in the general policy. Then the DNATed packets that are not matched by a VIP policy are matched with the general policy where they can be explicitly dropped and logged.

**Syntax:**

```
set match-vip {enable|disable}
```

**Default value:** disable

### diffserv-forward

Enables or disables application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, `diffservcode-forward` also needs to be configured.

**Syntax:**

```
set diffserv-forward {enable|disable}
```

**Default value:** disable

### diffserv-reverse

Enables or disables application of the differentiated services code point (DSCP) value to the DSCP field of reverse (reply) traffic. If enabled, `diffservcode-rev` also needs to be configured.

**Syntax:**

```
set diffserv-reverse {enable | disable}
```

**Default value:** disable

### diffservcode-forward

Used to set the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-forward` is enabled.

**Syntax:**

```
set diffservcode-forward <binary>
```

**Default value:** 000000

**Example:**

```
config firewall policy
    edit 0
        set diffservcode-forward 001001
    end
```

### diffservcode-rev

Used to set the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-rev` is enabled.

**Syntax:**

```
set diffservcode-rev <binary>
```

**Default value:** 000000

### tcp-mss-sender

Used to set the TCP Maximum Segment Size (MSS) number for the sender. When a FortiGate unit is configured to use PPPoE to connect to an ISP, certain web sites may not be accessible to users. This occurs because a PPPoE frame takes an extra 8 bytes off the standard Ethernet MTU of 1500. When the server sends the large packet with DF bit set to 1, the ADSL provider's router either does not send an "ICMP fragmentation needed" packet or the packet is dropped along the path to the web server. In either case, the web server never knows fragmentation is required to reach the client. Used to set the TCP Maximum Segment Size (MSS) number for the sender. When a FortiGate unit is configured to use PPPoE to connect to an ISP, certain web sites may not be accessible to users. This occurs because a PPPoE frame takes an extra 8 bytes off the standard Ethernet MTU of 1500. When the server sends the large packet with DF bit set to 1, the ADSL provider's router either does not send an "ICMP fragmentation needed" packet or the packet is dropped along the path to the web server. In either case, the web server never knows fragmentation is required to reach the client.

**Syntax:**

```
set tcp-mss-sender <integer>
```

### tcp-mss-receiver

Used to set the TCP MSS number for the receiver.

**Syntax:**

```
set tcp-mss-receiver <integer>
```

**Default value:** 0

### comments

Field to store descriptive information about the policy such as its intended purpose and targets. The field is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces.

**Syntax:**

```
set comments <string>
```

**Default value:** 0

**Example:**

```
config firewall policy
    edit 0
        set comments "Default outgoing traffic policy for corporate users"
    end
```

### label

Used to set a label for this policy. The label is visible in the GUI in Section View.

**Syntax:**

```
set label <string>
```

## global-label

Puts policy in the named subsection in the web-based manager. Subsection is created if it does not already exist.

### Syntax:

```
set global-label <string>
```

## auth-cert

Used to select an HTTPS server certificate for policy authentication. `self-sign` is the built-in, self-signed certificate; if you have added other certificates, you may select them instead. This field is available only if the `groups` or `users` fields are specified.

### Syntax:

```
set auth-cert <string>
```

## auth-redirect-addr

Used to set the IP address or domain name to redirect user HTTP requests after accepting the authentication disclaimer. The redirect URL could be to a web page with extra information (for example, terms of usage). To prevent web browser security warnings, this should match the CN field of the specified `auth-cert`, which is usually a fully qualified domain name (FQDN). This field is available only if the `groups` or `users` fields are specified.

### Syntax:

```
set auth-redirect-addr <string>
```

## redirect-url

Set the URL, if any, that the user is redirected to after authenticating and/or accepting the user authentication disclaimer. This field is available only if `disclaimer` is set to `enable`.

### Syntax:

```
set redirect-url <string>
```

## identity-based-route

Used to specify an identity-based route to be associated with the policy. Identity-based routes are defined in `firewall identity-based-route`.

### Syntax:

```
set identity-based-route <string>
```

## block-notification

Enables or disables the feature that displays the Fortinet Bar in the browser when a site is blocked and provides a block page via HTTP/HTTPS.

**Syntax:**

```
set block-notification {enable|disable}
```

**Default value:** disable

**custom-log-fields**

Used to enter log field index numbers to append one or more custom log fields to the log message for this policy. This option takes effect only if logging is enabled for the policy, and requires that you first define custom log fields. Separate multiple values with a space.

**Syntax:**

```
{set|append|clear} custom-log-fields <string> [<string> ...]
```

**tags**

Used to assign a custom tag to the firewall policy. The tags need to be preconfigured in `config system object-tag` and the same list of tags can be used anywhere that the tag setting is available. To see what tags are available for use, use the command `set tags ?`. Separate multiple values with a space.

**Syntax:**

```
{set|append|clear} tags <name_of_tag>
```

**Example:**

```
config system object-tag
    edit example-tag1
    next
    edit example-tag2
    next
    edit "example tag 3"
    next
end

config firewall policy
    edit 5
    set tags example-tag1 example-tag2
    append "example tag 3"
end
```

**replacemsg-override-group**

Used to select a replacement message override group from the available configured groups. This will override the default replacement message for this policy.

**Syntax:**

```
set replacemsg-override-group <string>
```



### srcaddr-negate

Enables or disables the negate source address match function. When enabled, this causes the `srcaddr` field to specify what the source address must **not** be.

#### Syntax:

```
set srcaddr-negate {enable|disable}
```

**Default value:** disable

### dstaddr-negate

Enables or disables the negate destination address match function. When enabled, this causes the `dstaddr` field to specify what the destination address must **not** be.

#### Syntax:

```
set dstaddr-negate {enable|disable}
```

**Default value:** disable

### service-negate

Enables or disables the negate service match function. When enabled, this causes the `service` field to specify what the service traffic must **not** be.

#### Syntax:

```
set service-negate {enable|disable}
```

**Default value:** disable

### timeout-send-rst

Enables or disables the sending of RST packet upon TCP session expiration.

#### Syntax:

```
set timeout-send-rst {enable|disable}
```

**Default value:** disable

### captive-portal-exempt

Enables or disables the exemption of users of this policy from the captive portal interface.

#### Syntax:

```
set captive-portal-exempt {enable|disable}
```

**Default value:** disable

## ssl-mirror

Enables or disables the SSL mirror function. This feature sends a copy of traffic decrypted by SSL inspection to one or more FortiGate interfaces so that it can be collected by raw packet capture tool for archiving and analysis. This feature is only available if the inspection mode is set do flow-based. Enables or disables the SSL mirror function. This feature sends a copy of traffic decrypted by SSL inspection to one or more FortiGate interfaces so that it can be collected by raw packet capture tool for archiving and analysis. This feature is only available if the inspection mode is set do flow-based.

### Syntax:

```
set ssl-mirror {enable|disable}
```

**Default value:** disable

## ssl-mirror-intf

Used to set the name of the SSL interface mirror. The value must be one of the existing interface names.

### Syntax:

```
{set|append|clear} ssl-mirror-intf <string> [<string> ...]
```

### Example:

```
config firewall policy
  edit 0
    set ssl-mirror-intf port11
  or ...
  set ssl-mirror-intf port12 port13
  or ...
  append ssl-mirror-intf port14
end
```

## scan-botnet-connections

Sets the scanning level traffic for connections to Botnet servers.

### Syntax:

```
set scan-botnet-connections {disable | block | monitor}
```

**Default value:** disable

## dsri

Enables or disables Disable Server Response Inspection (DSRI) which is used to assist performance when only using URL filtering as it allows the system to ignore the HTTP server responses.

### Syntax:

```
set dsri {enable|disable}
```

**Default value:** disable

### delay-tcp-npu-sessoin

Enables or disables the TCP NPU session delay in order to guarantee packet order of 3-way handshake.

#### Syntax:

```
set delay-tcp-npu-sessoin {enable|disable}
```

**Default value:** disable

## firewall schedule group

This command is used to configure schedule groups.

#### Syntax

```
config firewall schedule group {edit|delete|purge|rename|get|show}
```

## Managing schedule group objects

The configuration of specific schedule group objects is the most common activity when using the `config firewall schedule group` command but some commands affect the address objects as a whole.

### edit

Used to select which individual schedule group to configure or edit values.

```
edit <schedule group>
```

To get a list of all of the existing schedule group objects, type the command:

```
Command Prompt (group) # edit ?
```

If you are creating a new schedule group object, just type the name you wish to used after the edit command. If there are spaces in the name, use quotation marks.

### delete

Used to delete an existing schedule object

```
delete
```

The can be a string of up to 64 characters.

### purge

Used delete all of the existing schedule group objects. It deletes all of the values within the table that holds the information about schedule group objects within the VDOM.

```
purge
```

There are no options, parameters or qualifiers. Just use the enter key after entering the command This command has a serious impact. Use cautiously.

## rename

Used to change the name of the schedule group object.

```
rename <schedule group> to <schedule group>
```

## Options and settings within a Schedule Group

### name

This field is a unique name given to represent the schedule group object. This setting is first defined when using the edit command to edit a category that does not currently exist. The name field of a schedule group object cannot be changed from within the object. It can be changed by using the rename command in the config firewall schedule group context.

### member

Defines the schedule objects that are members of the schedule group. The value is a that should be the name of one of the existing schedule objects configured on the device. A group cannot contain other groups Separate multiple interfaces with spaces.

#### Syntax:

```
{set|append} members <schedule group>[ ...]
```

#### Example:

```
config firewall schedule group
  edit example_group
  set member example_schedule1
  or ...
  set member example_schedule1 example_schedule2
  or ...
  append example_schedule3
end
```

### color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1.

#### Syntax:

```
set color <integer>
```

#### Default value: 0

#### Example:

```
config firewall schedule group
  edit generic-schedule group-name
  set color 15
end
```

## firewall schedule onetime

This command is used to add, edit, delete or rename one-time schedules.

Schedule objects are used to control when policies are active or inactive. The one-time schedule is for policies that are effective once for a specified period of time and then not used again.

### Syntax

```
config firewall schedule onetime {edit|delete|purge|rename|get|show}
```

## Managing service group objects

The configuration of a specific onetime schedule object is the most common activity when using the `config firewall schedule onetime` command but some commands affect the schedule objects as a whole.

### edit

Used to select which individual schedule to configure or edit values.

```
edit <onetime schedule>
```

To get a list of all of the existing service group objects, type the command:

```
Command Prompt (onetime) # edit ?
```

If you are creating a new onetime schedule object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

### delete

Used to delete an existing onetime schedule

```
delete <onetime schedule>
```

- The `<onetime schedule>` can be a string of up to 64 characters.

## purge

Used to delete all of the existing onetime schedule objects. It deletes all of the values within the table that holds the information about service group objects within the VDOM.

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

### rename

Used to change the name of the onetime schedule object.

```
rename <onetime schedule> to <new_onetime_schedule>
```

## Options and settings within a onetime schedule

### name

This field is a unique name given to represent the onetime schedule object. This setting is first defined when using the edit command to edit a category that does not currently exist. The name field of a onetime schedule object cannot be changed from within the object. It can be changed by using the rename command in the `config firewall schedule onetime` context.

### start

This field is for specifying the starting date and time of the schedule object.

#### Syntax:

<hh:mm> <yyyy/mm/dd>

- hh - hours in the 24-hour clock: 00 to 23
- mm - Minutes in quarter hour increments: 15, 30, or 45
- yyyy - Year, the range being: 2001-2050
- mm - Months: 01 to 12
- dd - Day of the month: 01 to 31

**Default value:** 00:00 2001/01/01

### end

Enter the ending day and time of the schedule.

#### Syntax:

<hh:mm> <yyyy/mm/dd>

- hh - hours in the 24-hour clock: 00 to 23
- mm - Minutes in quarter hour increments: 15, 30, or 45
- yyyy - Year, the range being: 2001-2050
- mm - Months: 01 to 12
- dd - Day of the month: 01 to 31

**Default value:** 00:00 2001/01/01

#### Example of setting the times

- Set the start time to 1:30 p.m. on August 4, 2018
- Set the end time to 12:45 a.m. on August 31, 2018

```
config firewall schedule onetime
edit schedule1
set start 13:30 2018/08/04
set end 00:45 2018/08/31
end
```

## color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1.

### Syntax

```
set color <integer>
```

**Default value:** 0

### Example:

```
config firewall schedule onetime
    edit schedule1
        set color 15
    end
```

## expiration-days

This field specifies how many days before the expiration of the schedule an event log will be generated in order to warn of the impending cancellation of the schedule. The content of the field is an integer. To generate an event, the range is 1 to 100 days. To disable the generation of the event log, enter 0.

### Example

```
config firewall schedule onetime
    edit schedule1
        set expiration-days 5
    end
```

**Default value:** 3

## firewall service category

Use this command to create new categories or add comments to firewall service categories. To assign services to categories, use the `firewall service custom` command. The adding or editing the name of a service category are the most common tasks when using the `config firewall service category` command but some commands affect the address objects as a whole.

## edit

Used to add an additional category or select which individual category to edit.

### Syntax:

```
edit <category_name>
```

To create a new service category, just type the `category_name` you wish to use after the `edit` command. A new category will be created using the `category_name` supplied. If you require spaces in the name you can:

- Use quotation marks around the entire `category_name`
- Use the escape character before the space character. Example: for the `category_name` `Web Access` type `Web\ Access`

To get a list of all of the existing categories, type the command:

```
Command Prompt (category) # edit ?
```

## delete

Used to delete an existing category

### Syntax:

```
delete <category_name>
```

## purge

Used delete all of the existing categories. It deletes all of the values within the table that holds the categories.

### Syntax:

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

## rename

Used to change the name of the category.

### Syntax:

```
rename <category_name> to <new_category_name>
```

## move

Used to move the position of a category, relative to another category, in the order of their listing.

### Syntax:

```
move <category_name> {after | before} <category_name>
```

## clone

Used to copy all of the attributes of an existing category to a new category.

### Syntax:

```
clone <category_name> to <category_name>
```



## name

This field is a unique name given to represent the address object. This setting is first defined when using the `edit` command to edit a category that does not currently exist. The name field of an address object cannot be changed from within the object. It can be changed by using the `rename` command in the `config firewall service category` context.

## comment

Field used to store descriptive information about the category such as the type of services that should be included in the category. Enclose the string in quotes to enter special characters or spaces.

### Syntax:

```
set comment <string>
```

### Example:

```
config firewall service category
  edit "Custom Category"
    set comment "For services that are proprietary to the company."
end
```

## firewall service custom

This command is used to configure firewall services.

## Managing service objects

The configuration of specific service is the most common activity when using the `firewall policy` command but some commands affect the service objects as a whole.

### edit

Used to select which individual service to configure or edit values.

### Syntax:

```
config firewall service custom
(custom) # edit <service>
```

- To get a list of all of the existing address objects, type the command:

```
(custom) # edit ?
```

If you are creating a new service object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

## delete

Used to delete an existing service

### Syntax:

```
config firewall service custom
(custom) # delete <service>
```

## purge

Used to delete all of the existing firewall policies. It deletes all of the values within the table within the VDOM.

### Syntax:

```
config firewall service custom
(custom) # purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

## rename

Used to change the name of the service object.

```
config firewall service custom
(custom) # rename <service_name> to <new_service_name>
```

## Options and settings within a service

### explicit-proxy

Enable to configure this service as an explicit web proxy service. The service will be available to explicit proxy firewall policies but not to regular firewall policies.

### Syntax

```
set explicit-proxy {enable | disable}
```

**Default value:** disable

### category

Assign the service to a service category. These categories are created and managed using the command `firewall service`.

### Syntax

```
set category <category_name>
```

### Example

```
config firewall services custom
(custom) # edit sample_service
```

```
(sample_service) # set category "web services"
(sample_service) # end
```

## protocol

Select the protocol used by the service. These protocols are available when `explicit-proxy` is disabled. If you select TCP/UDP/SCTP you must specify the `tcp-portrange`, `udp-portrange`, or `sctp-portrange`.

### Syntax

```
set protocol {ICMP | ICMP6 | IP | TCP/UDP/SCTP}
```

**Default value:** TCP/UDP/SCTP A different set of protocols are available when `explicit-proxy` is enabled.

```
set protocol {ALL | CONNECT | FTP | HTTP | SOCKS-TCP | SOCKS-UDP}
```

**Default value:** ALL

### Example

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set explicit-proxy enable
    (sample-service) # set protocol FTP
(sample-service) # end
```

## iprange

Enter an IP address or address range for this service.

### Syntax

```
set iprange <ip_address[<-<ip_address>]>>
```

**Default value:** 0.0.0.0

### Example

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set iprange 192.168.0.64-192.168.0.128
(sample-service) # end
```

## fqdn

Enter a fully-qualified domain name (FQDN) for this service.

### Syntax

```
set fqdn <fqdn_str>
```

**Example**

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set fqdn example.com
(sample-service) # end
```

**protocol-number (0,4294967295)**

For an IP service, enter the IP protocol number. For information on protocol numbers, see <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>.

**Syntax**

```
set protocol-number <protocol_int>
```

**Default value:** 0

**Example**

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set protocol-number 6
(sample-service) # end
```

**icmptype**

Enter the ICMP type number. The range for type\_int is from 0-255. Find ICMP type and code numbers at <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-types>.

**Syntax**

```
set icmptype <type_int>
```

**Example**

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set icmptype 8
(sample-service) # end
```

**icmpcode**

Enter the ICMP code number. Find ICMP type and code numbers at <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-types>.

**Syntax**

```
set icmpcode <code_int>
```

## Example

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set icmpcode 13
(sample-service) # end
```

## tcp-portrange

For TCP services, enter the destination and source port ranges.

- If the destination port range can be any port, enter 0-65535.
- If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`.
- If the source port can be any port, no source port need be added.
- If source port can be any port, no source port need be added.
- If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.

The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.

## Syntax

```
set tcp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<src-  
porthigh_int>]
```

## Example

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set tcp-portrange 100-150:1100-1150
(sample-service) # end
```

or if multiple ranges, separate the ranges with a space.

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set tcp-portrange 100-150:1100-1150 2000-2100:4000:4100
(sample-service) # end
```

## udp-portrange

For UDP services, enter the destination and source port ranges.

- If the destination port range can be any port, enter 0-65535.
- If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`.
- If source port can be any port, no source port need be added.
- If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.

The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.

### Syntax

```
set udp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<src-  
porthigh_int>]
```

### sctp-portrange

For SCTP services, enter the destination and source port ranges.

- If the destination port range can be any port, enter 0-65535.
- If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`.
- If source port can be any port, no source port need be added.
- If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.

The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.

### Syntax

```
set sctp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<src-  
porthigh_int>]
```

### tcp-halfclose-timer (0,86400)

Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in `system global`. This is available when protocol is TCP/UDP/SCTP.

### Syntax

```
set tcp-halfclose-timer <seconds>
```

**Default value:** 0

### Example:

```
config firewall service custom  
    (custom) # edit sample-service  
        (sample-service) # set tcp-halfclose-timer 3600  
    (sample-service) # end
```

### tcp-halfopen-timer (0,86400)

Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in `system global`. This is available when protocol is TCP/UDP/SCTP.

### Syntax

```
set tcp-halfopen-timer <seconds>
```

**Default value:** 0

## tcp-timewait-timer

Set the length of the TCP TIME-WAIT state in seconds. As described in [RFC 793](#), the “TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request”. Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Enter 0 to use the global setting defined in system global. This is available when protocol is TCP/UDP/SCTP.

### Syntax

```
set tcp-timewait-timer <seconds_int>
```

**Default value:** 0

### Example:

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set tcp-timewait-timer 60
    (sample-service) # end
```

## udp-idle-timer

Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in system global. This is available when protocol is TCP/UDP/SCTP.

### Syntax

```
set udp-idle-timer <seconds>
```

**Default value:** 0

## session-ttl

Enter the default session timeout in seconds. The valid range is from 300 - 604,800 seconds. Enter 0 to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. This is available when protocol is TCP/UDP/SCTP.

### Syntax

```
set session-ttl <seconds>
```

**Default value:** 0

### Example:

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set session-ttl 3600
    (sample-service) # end
```

## check-reset-range

Configure ICMP error message verification.

- `disable` — The FortiGate unit does not validate ICMP error messages.
- `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If `log-invalid-packet` is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the anti-replay option checks packets.
- `default` — Use the global setting defined in system global.

This field is available when protocol is TCP/UDP/SCTP. This field is not available if explicit-proxy is enabled.

### Syntax

```
set check-reset-range {disable | strict | default}
```

**Default value:** default

## comment

Field to store descriptive information about the service such as its intended purpose.

### Syntax

```
set comment <string>
```

## color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1. This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1.

### Syntax

```
set color <integer>
```

**Default value:** 0

### Example:

```
config firewall service custom
    edit generic-custom-service
        set color 15
end
```

## visibility

Enable visibility to include this service in firewall policy service selection.

### Syntax

```
set visibility {enable | disable}
```

**Default value:** enable



## firewall vip

Configure firewall virtual IPs (VIPs) and their associated addresses and port mappings (NAT). Use VIPs to configure destination NAT and server load balancing. For information about FortiOS Firewall VIPs in general, see [Virtual IPs](#). For information about server load balancing with FortiOS Firewall VIPs see [Server Load Balancing](#).

### uuid

Each VIP has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited.

### comment <comment>

Add a comment about the VIP.

### type {dns-translation | load-balance | server-load-balance | static-nat}

Select the type of static or dynamic NAT applied by the virtual IP.

- `dns-translation` dynamic VIP with DNS translation.
- `load-balance` dynamic NAT load balancing with server selection from an IP address range.
- `server-load-balance` dynamic NAT load balancing with server selection from among up to eight real servers, determined by your selected load balancing algorithm and server responsiveness monitors. Includes SSL offloading.
- `static-nat` Static NAT (the default).
- `fqdn` dynamic fully qualified domain name (FQDN) VIP.

### ldb-method {first-alive | http-host | least-rtt | least-session | round-robin | static | weighted}

Select the method used by the virtual server to distribute sessions to the real servers. You add real servers to the virtual server using `config real servers`.

This option appears only if `type` is `server-loadbalance`.

`first-alive` Always directs requests to the first alive real server. In this case “first” refers to the order of the real servers in the virtual server configuration. For example, if you add real servers A, B and C in that order, then traffic always goes to A as long as it is alive. If A goes down then traffic goes to B and if B goes down the traffic goes to C. If A comes back up, traffic goes to A. Real servers are ordered in the virtual server configuration in the order in which you add them, with the most recently added real server last. If you want to change the order you must delete and re-add real servers as required.

`http-host` Load balance HTTP requests by the contents of the HOST header.

`least-rtt` Directs requests to the real server with the least round trip time. The round trip time is determined by a Ping monitor and is defaulted to 0 if no Ping monitors are defined.

`least-session` Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing have similar capabilities.

`round-robin` Directs request to the next real server, and treats all real servers as equals regardless of response time or number of connections. Unresponsive real servers are avoided. A separate real server is required.

`static` (the default) Distributes sessions evenly across all real servers according to the session source IP address. This load balancing method provides some persistence because all sessions from the same source address would always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not required. (the default) Distributes sessions evenly across all real servers according to the session source IP address. This load balancing method provides some persistence because all sessions from the same source address would always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not required.

`weighted` Real servers with a higher weight value receive a larger percentage of connections at any one time. Server weights can be set in `config realservers set weight`.

## dns-mapping-ttl

Enter time-to-live for DNS response. Range 0 to 604 800. Available when type is `dns-translation`. Default is 0 which means use the DNS server's response time.

## src-filter <address> [<address>...]

Enter a source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y). Separate addresses by spaces.

## extip <address>[-<address>]

Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network. If type is `static-nat` and `mappedip` is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. To configure a dynamic virtual IP that accepts connections destined for any IP address, set `extip` to 0.0.0.0.

## mappedip <address> [<address>...]

Enter the IP address or IP address range on the destination network to which the external IP address is mapped. If type is `static-nat` and `mappedip` is an IP address range, FortiOS uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. If type is `load-balance` and `mappedip` is an IP address range, the FortiGate unit uses `extip` as a single IP address to create a one-to-many mapping. Input each address (separated by spaces) in the format of IP (x.x.x.x), IP subnet (x.x.x.x/y) or IP range (x.x.x.x-y.y.y.y).

## extintf <name>

Enter the name of the interface connected to the source network that receives the packets that will be forwarded to the destination network. The interface name can be any FortiGate network interface, VLAN subinterface, IPSec VPN interface, or modem interface.

## arp-reply {disable | enable}

Enable to respond to ARP requests for this virtual IP address. Enabled by default.

## server-type {http | https | imaps | ip | pop3s | smtps | ssl | tcp | udp}

If the type is `server-load-balance`, select the protocol to be load balanced by the virtual server (also called the server load balance virtual IP). If you select a general protocol such as `ip`, `tcp`, or `udp` the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as `http`, `https`, or `ssl` you can apply additional server load balancing features such as persistence and HTTP multiplexing.

- `http` load balance only HTTP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 80 for HTTP sessions). You can also configure `httpmultiplex`. You can also set persistence to `http-cookie` and configure `http-cookiedomain`, `http-cookie-path`, `http-cookiegeneration`, `http-cookie-age`, and `httpcookie-share` settings for cookie persistence.
- `https` load balance only HTTPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 443 for HTTPS sessions). You can also configure `httpmultiplex` and set persistence to `httpcookie` and configure the same `http-cookie` options as for `http` virtual servers plus the `httpscookie-secure` option. You can also set persistence to `ssl-session-id`. You can also configure the SSL options such as `ssl-mode` and `ssl-certificate` and so on. `https` is available on FortiGate units that support SSL acceleration.
- `imaps` load balance only IMAPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 993 for IMAPS sessions).
- `ip` load balance all sessions accepted by the firewall policy that contains this server load balance virtual IP. Since all sessions are load balanced you don't have to set the `extport`.
- `pop3s` load balance only POP3S sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 995 for POP3S sessions).
- `smtps` load balance only SMTPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 465 for SMTPS sessions).
- `ssl` load balance only SSL sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced. You can also configure the SSL options such as `ssl-mode` and `ssl-certificate` and so on.
- `tcp` load balance only TCP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced.
- `udp` load balance only UDP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced.

## persistence {none | http-cookie | ssl-session-id}

If the type is `server-load-balance`, configure persistence for a virtual server to make sure that clients connect to the same server every time they make a request that is part of the same session. When you configure persistence, the FortiGate load balances a new session to a real server according to the `ldb-method`. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server. Persistence is disabled by default. You can

configure persistence if . If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server. Persistence is disabled by default. You can configure persistence if `server-type` is set to `http`, `https`, or `ssl`.

- `none` No persistence. Sessions are distributed solely according to the `ldb-method`. Setting `ldbmethod` to `static` (the default) results in behavior equivalent to persistence.
- `http-cookie` all HTTP or HTTPS sessions with the same HTTP session cookie are sent to the same real server. `http-cookie` is available if `server-type` is set to `https` or `ssl`. If you select this option you can also configure `httpcookie-domain`, `http-cookie-path`, `httpcookie-generation`, `http-cookie-age`, and `http-cookie-share` for HTTP and these settings plus `https-cookie-secure` for HTTPS.
- `ssl-session-id` all sessions with the same SSL session ID are sent to the same real server. `sslsession-id` is available if `server-type` is set to `https` or `ssl`.

### nat-source-vip {disable | enable}

Enable (the default) to prevent unintended servers from using a virtual IP. The virtual IP will be used as the source IP address for connections from the server through the FortiGate.

Disable to use the actual IP address of the server (or the FortiGate destination interface if using NAT) as the source address of connections from the server that pass through the FortiGate unit.

### portforward {disable | enable}

Select to enable port forwarding. You must also specify the port forwarding mappings by configuring `extport` and `mappedport`. Disabled by default.

### protocol {sctp | tcp | udp | icmp}

Select the protocol to use when forwarding packets. The default is `tcp`.

### extport <port-number>

External port number range that you want to map to a port number range on the destination network.

This option only appears if `portforward` is enabled. If `portforward` is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set `extport` to the port number range. Then set `mappedport` to the start and end of the destination port range.

When using port number ranges, the external port number range corresponds to a mapped port number range containing an equal number of port numbers, and each port number in the external range is always translated to the same port number in the mapped range.

If `type` is `server-load-balance`, `extport` is available unless `server-type` is `ip`. The value of `extport` changes to 80 if `server-type` is `http` and to 443 if `server-type` is `https`.

### config realservers

The following are the options for `config realservers`, and are available only if `type` is `server-load-balance`.

### ip <server-ip>

Enter the IP address of a server in this server load balancing cluster.

### port

Enter the port used if port forwarding is enabled.

### status {active | disable | standby}

Select whether the server is in the pool of servers currently being used for server load balanced traffic, the server is on standby, or is disabled. Default is `active`.

- `active` The FortiGate unit may forward traffic to the server unless its health check monitors determine that the server is unresponsive, at which time the FortiGate unit temporarily uses a server whose `status` is `standby`. The healthcheck monitor will continue to monitor the unresponsive server for the duration of `holddown-interval`. If this server becomes reliably responsive again, it will be restored to active use, and the standby server will revert to standby.
- `disable` The FortiGate unit does not forward traffic to this server, and does not perform health checks. You might use this option to conserve server load balancing resources when you know that a server will be unavailable for a long period, such as when the server is down for repair.
- `standby` If a server whose `status` is `active` becomes unresponsive, the FortiGate temporarily uses a responsive server whose `status` is `standby` until the server whose `status` is `active` again becomes reliably responsive. If multiple responsive `standby` servers are available, the FortiGate selects the standby server with the greatest weight. If a standby server becomes unresponsive, the FortiGate selects another responsive server whose `status` is `standby`.

### holddown-interval <interval>

Enter the amount of time in seconds that the health check monitor continues to monitor the status of a server whose status is active after it has been detected to be unresponsive. Default is 300 seconds. If the server is detected to be continuously responsive during this interval, a server whose status is standby is removed from current use and replaced with this server, which is then used by server load balanced traffic. In this way, server load balancing prefers to use active servers, if they are responsive. If the server is detected to be unresponsive during the first holddown interval, the server remains out of use for server load balanced traffic, the health check monitor will double the holddown interval once, and continue to monitor the server for the duration of the doubled holddown interval. The health check monitor continues to monitor the server for additional iterations of the doubled holddown interval until connectivity to the server becomes reliable, at which time the holddown interval reverts to the configured interval, and the newly responsive active server replaces the standby server in the pool of servers currently in use. In effect, if the status of a server is active but the server is habitually unresponsive, the health check monitor is less likely to restore the server to use by server load balanced traffic until the server's connectivity becomes more reliable. This option applies only to real servers whose status is active, but have been detected to be unresponsive or down.

### healthcheck {disable | enable}

Enable to check the responsiveness of the server before forwarding traffic. You must also configure `monitor`. Disabled by default.

### max-connections <number>

Enter the limit on the number of active connections directed to a real server. If the maximum number of connections is reached for the real server, the FortiGate unit will automatically switch all further connection requests to another server until the connection number drops below the specified limit. The default of 0 means unlimited connections.

### client-ip <ip\_range\_ipv4> [<ip\_range\_ipv4>] [<ip\_range\_ipv4>] [<ip\_range\_ipv4>]

Restrict the clients that can connect to a real server according to the client's source IP address. Use the `client-ip` option to enter up to four client source IP addresses or address ranges. Separate each IP address or range with a space. The following example shows how to add a single IP address and an IP address range:

```
set client-ip 192.168.1.90 192.168.1.100-192.168.1.120
```

Use the `client-ip` option if you have multiple real servers in a server load balance VIP and you want to control which clients use which real server according to the client's source IP address. Different real servers in the same virtual server can have the same or overlapping IP addresses and ranges. If an overlap occurs, sessions from the overlapping source addresses are load balanced among the real servers with the overlapping addresses. If you do not specify a `client-ip` all clients can use the real server.

### weight <weight>

Enter the weight value of a specific server. Servers with a greater weight receive a greater proportion of forwarded connections, or, if their `status` is `standby`, are more likely to be selected to temporarily replace servers whose `status` is `active`, but that are unresponsive. Valid weight values are between 1 and 255. Default is 1. This option is available only if `ldb-method` is `weighted`.

### mappedport <port>

Enter the port number range on the destination network to which the external port number range is mapped. You can also enter a port number range to forward packets to multiple ports on the destination network.

### gratuitous-arp-interval <time>

Configure sending of gratuitous ARP packets by a virtual IP. You can set the time interval between sending the packets. The default is 0, which disables this feature.

### srcintf-filter <interface> [<interface>...]

Enter names of the interfaces to which the VIP applies. Separate names with spaces.

### http-cookie-domain-from-host {enable | disable}

If enabled, when the FortiGate unit adds a SetCookie to the HTTP(S) response, the Domain attribute in the SetCookie is set to the value of the Host: header, if there was one. If there was no Host: header, the Domain attribute is set to the value of `http-cookie-domain` if it is set and if it is not then the Domain attribute will not be included in the SetCookie. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http-cookie`. Enabled by default.

### http-cookie-domain <domain>

Configure HTTP cookie persistence to restrict the domain that the cookie should apply to. Enter the domain name to restrict the cookie to. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

### http-cookie-path <path>

Configure HTTP cookie persistence to limit the cookies to a particular path, for example `/new/path`. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

### http-cookie-generation <generation>

Configure HTTP cookie persistence to invalidate all cookies that have already been generated. The exact value of the generation is not important, only that it is different from any generation that has already been used. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

### http-cookie-age <age>

Configure HTTP cookie persistence to change how long the browser caches the cookie. Enter an age in minutes or set the age to 0 to make the browser keep the cookie indefinitely. The range is 0 to 525600 minutes. The default age is 60 seconds. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

### http-cookie-share {disable | same-ip}

Configure HTTP cookie persistence to control the sharing of cookies across more than one virtual server. The default setting `same-ip` means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain. `Disable` to make sure that a cookie generated for a virtual server cannot be used by other virtual servers. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

### https-cookie-secure {disable | enable}

Configure HTTP cookie persistence to enable or disable using secure cookies for HTTPS sessions. Secure cookies are disabled by default because they can interfere with cookie sharing across HTTP and HTTPS virtual servers. If enabled, then the `Secure` tag is added to the cookie inserted by the FortiGate unit. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

### http-multiplex {disable | enable}

Enable to use the FortiGate to multiplex multiple client connections into a few connections between the FortiGate and the real server. This can improve performance by reducing server overhead associated with establishing multiple connections. The server must be HTTP/1.1 compliant. Disabled by default. This option is only available if `server-type` is `http` or `https`.

## http-ip-header {disable | enable}

In HTTP multiplexing is enabled, set `http-ip-header` to `enable` to add the original client IP address in the `XForwarded-For` HTTP header. This can be useful in an HTTP multiplexing configuration if you want to be able to see the original client IP address in log messages on the destination web server. If this option is disabled, the HTTP header. This can be useful in an HTTP multiplexing configuration if you want to be able to see the original client IP address in log messages on the destination web server. If this option is disabled, the `XForwarded-For` header will contain the IP address of the FortiGate unit. Disabled by default. If enabled the `http-ip-header-name` option appears and you can specify a different header to add the client IP address to. This option appears only if `type` is `server-load-balance`, `server-type` is `http` or `https` and `http-multiplex` is enabled.

## http-ip-header-name <name>

In an HTTP multiplex configuration, if you enable `http-ip-header` you can use the `http-ip-header-name` option to add the original client IP address to a custom http header. Use this option to specify the name of the header to add the IP address to. The destination server extracts the original client IP address from this header to record log messages that include client IP addresses. If you leave this option blank (the default) the original client IP address is added to the `XForwarded-For` header. This option appears only if `type` is `server-load-balance`, `server-type` is `http` or `https` and `http-multiplex` is enabled and `http-ip-header` is enabled.

## outlook-web-access {disable | enable}

If the FortiGate unit provides SSL offloading for Microsoft Outlook Web Access then the Outlook server expects to see a `Front-End-Https: on` header inserted into the HTTP headers as described in this [Microsoft Technical Note](#). If `outlook-web-access` is enabled the FortiGate adds this header to all HTTP requests. Disabled by default. This options is available when `type` is `server-load-balance` is enabled and `server-type` is `http` or `https`.

## weblogic-server {disable | enable}

Enable or disable adding an HTTP header to indicate SSL offloading for a WebLogic server. Disabled by default.

## websphere-server {disable | enable}

Enable or disable adding an HTTP header to indicate SSL offloading for a WebSphere server. Disabled by default.

## ssl-mode {full | half}

Select whether or not to accelerate SSL communications with the destination by using the FortiGate to perform SSL operations, and indicate which segments of the connection will receive SSL offloading. Accelerating SSL communications in this way is also called SSL offloading.

- `half` (the default) apply SSL acceleration only between the client and the FortiGate. The segment between the FortiGate and the server is clear text. This results in better performance, but cannot be used in failover configurations where the failover path does not have an SSL accelerator.



- **full** apply SSL acceleration to both parts of the connection: the segment between the client and the FortiGate, and the segment between the FortiGate and the server. The segment between the FortiGate and the server is encrypted, but the handshakes are accelerated. This results in performance which is less than if `ssl-mode` is set to **half**, but still improved over no SSL acceleration, and can be used in failover configurations where the failover path does not have an SSL accelerator. If the server is already configured to use SSL, this also enables SSL acceleration without requiring changes to the server's configuration. If this option is set to **full** then several `ssl-server` options appear and you can apply different SSL features (such as encryption levels) to the client connection and to the server connection.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

## ssl-certificate <name>

The name of the SSL certificate to use for SSL acceleration. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to **full**, the same certificate is used for client and server communication.

## ssl-dh-bits <bits>

Enter the number of bits used in the Diffie-Hellman exchange for RSA encryption of the SSL connection. Larger prime numbers are associated with greater cryptographic strength. Default is 2048. Values include 768, 1024, 1536, 2048, 3072, and 4096. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to **full**, the `ssl-dh-bits` setting is used for client and server communication.

## ssl-algorithm {high | medium | low | custom}

Set the permitted encryption algorithms for SSL sessions according to encryption strength.

- **high** (the default) permit only high encryption algorithms: AES or 3DES.
- **medium** permit high (AES, 3DES) or medium (RC4) algorithms.
- **low** permit high (AES, 3DES), medium (RC4), or low (DES) algorithms.
- **custom** only allow some cipher suites to be used. Use `config ssl-cipher-suites` to select the cipher suites that are allowed.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to **full** and `ssl-server-algorithm` is set to `client`, the `ssl-algorithm` setting applies to both client and server communication. If `ssl-server-algorithm` is not set to `client`, the `ssl-algorithm` setting only applies to client communication. You can use the `ssl-server-algorithm` option to select different algorithms for server communication.

## config ssl-cipher-suites

Choose one or more SSL cipher suites to use for SSL sessions. Only available if `ssl-algorithm` is set to `custom`. You can also use this command to list the supported SSL cipher suites available to all FortiOS SSL encryption/decryption applications.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to **full** and `ssl-server-algorithm` is set to `client`, the configured setting applies to both client and server communication.

If `ssl-server-algorithm` is not set to `client`, the `config ssl-cipher-suites` configuration only applies to client communication. You can use `config ssl-cipher-suites` to select different cipher suites for server communication.

### **cipher <cipher-suite-name>**

Set the cipher suite name to use. Use `?` to list the available cipher suite names.

### **versions {ssl-3.0 | tls-1.0 | tls-1.1}**

Select the SSL/TLS versions that are supported.

## **ssl-server-algorithm {high | medium | low | custom}**

Set the permitted encryption algorithms for SSL server sessions according to encryption strength.

- `high` (the default) permit only high encryption algorithms: AES or 3DES.
- `medium` permit high (AES, 3DES) or medium (RC4) algorithms.
- `low` permit high (AES, 3DES), medium (RC4), or low (DES) algorithms.
- `custom` only allow some cipher suites to be used. Use `config ssl-server-cipher-suites` to select the cipher suites that are allowed.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-mode` is `full`.

## **config ssl-server-cipher-suites**

Choose one or more SSL cipher suites to use for SSL server sessions. Only available if `ssl-server-algorithm` is set to `custom`. You can also use this command to list the supported SSL cipher suites available to all FortiOS SSL encryption/decryption applications.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, `ssl-mode` is `full`, and `ssl-server-algorithm` is `custom`.

### **cipher <cipher-suite-name>**

Set the cipher suite name to use. Use `?` to list the available cipher suite names.

### **versions {ssl-3.0 | tls-1.0 | tls-1.1}**

Select the SSL/TLS versions that are supported.

## **ssl-pfs {allow | deny | require}**

Select handling of perfect forward secrecy (PFS) by controlling the cipher suites that can be selected. Applies to both client and server sessions.

- `allow` allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.
- `deny` allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.
- `require` allow only Diffie-Hellman cipher-suites, so PFS is applied.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-algorithm` is not set to `custom`.

### ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}

The lowest version of SSL/TLS to allow in SSL sessions. Default is `tls-1.0`. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full` and `ssl-server-min-version` is set to `client`, the configured setting applies to both client and server communication. If `ssl-server-min-version` is not set to `client`, this option only applies to client communication.

### ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}

The highest version of SSL/TLS to allow in SSL sessions. Default is `tls-1.2`. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full` and `ssl-server-max-version` is set to `client`, the configured setting applies to both client and server communication. If `ssl-server-max-version` is not set to `client`, this option only applies to client communication.

### ssl-server-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | client}

The lowest version of SSL/TLS to allow in SSL server sessions. Default is `client` which means the `ssl-min-version` applies to both client and server sessions. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-mode` is set to `full`.

### ssl-server-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | client}

The highest version of SSL/TLS to allow in SSL server sessions. Default is `client` which means the `ssl-max-version` applies to both client and server sessions. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-mode` is set to `full`.

### ssl-send-empty-frags {disable | enable}

Select to precede the record with empty fragments to thwart attacks on CBC IV. You might disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments. Enabled by default. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and applies only to SSL 3.0 and TLS 1.0.

### ssl-client-fallback {disable | enable}

Enable (the default) to prevent Downgrade Attacks on client connections ([RFC 7507](#)). This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

### ssl-client-renegotiation {allow | deny | secure}

Select the SSL secure renegotiation policy. Secure renegotiation complies with [RFC 5746](#) Secure Negotiation Indication. The vulnerability [CVE-2009-3555](#) affects all SSL/TLS servers that support re-negotiation. FortiOS when configured for SSL/TLS offloading is operating as a SSL/TLS server. The IETF is working on a TLS protocol change that will fix the problem identified by [CVE-2009-3555](#) while still supporting re-negotiation. Until that protocol change is available, you can use the `ssl-client-renegotiation` option to disable support for SSL/TLS re-negotiation.

- `allow` (the default) allow, but do not require secure renegotiation.
- `deny` do not allow renegotiation.
- `secure` require secure renegotiation.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

### **ssl-client-session-state-type {both | client | disable | time}**

The method the FortiGate should use to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.

- `both` (the default) expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first.
- `count` expire SSL session states when `ssl-client-session-state-max` is exceeded.
- `disable` expire all SSL session states.
- `time` expire SSL session states when `ssl-client-session-state-timeout` is exceeded.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

### **ssl-client-session-state-timeout <timeout>**

The number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the FortiGate unit. Default is 30 minutes. Range is 1 to 14400. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

### **ssl-client-session-state-max <states>**

The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit. Default is 1000. Range is 0 to 100000. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

### **ssl-server-session-state-type {both | count | disable | time}**

The method the FortiGate should use to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.

- `both` (the default) expire SSL session states when either `ssl-server-session-state-max` or `ssl-server-session-state-timeout` is exceeded, regardless of which occurs first.
- `count` expire SSL session states when `ssl-server-session-state-max` is exceeded.
- `disable` expire all SSL session states.
- `time` expire SSL session states when `ssl-server-session-state-timeout` is exceeded.

This option appears only if `ssl-mode` is `full`.

### **ssl-server-session-state-timeout <time>**

The number of minutes to keep the SSL session states for the segment of the SSL connection between the server and the FortiGate. Default is 30 minutes. Range is 1 to 14400. This option appears only if `ssl-mode` is `full`.

## ssl-server-session-state-max

The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit. Default is 1000. Range is 0 to 100000. This option appears only if `ssl-mode` is `full`.

## ssl-http-location-conversion {disable | enable}

Select to replace `http` with `https` in the reply's `Location` HTTP header field. For example, the reply, `Location: http: //example.com/` would be converted to `Location: https://example.com/`. Disabled by default. This option appears only if `type` is `server-loadbalance` and `server-type` is `https`.

## ssl-http-match-host {disable | enable}

Enable to apply Location conversion to the reply's HTTP header only if the host name portion of `Location` matches the request's `Host` field, or, if the `Host` field does not exist, the host name portion of the request's URI. If this option is disabled (the default), conversion occurs regardless of whether the host names in the request and the reply match. For example, if `ssl-http-match-host` is enabled, and a request contains `Host: example.com` and the reply contains `Location: http://example.cc/`, the `Location` field does not match the `Host` field of the original request and the reply's `Location` field remains unchanged. If the reply contains `Location: http://example.com/`, however, then the FortiGate detects the matching host name and converts the reply field to `Location: https://example.com/`. This option appears only if `type` is `server-loadbalance` and `server-type` is `https` and `ssl-http-location-conversion` is `enable`.

## monitor <name>

The name of the health check monitor for use when polling to determine a virtual server's connectivity status.

## max-embryonic-connections <number>

The maximum number of partially established SSL or HTTP connections. This should be greater than the maximum number of connections you want to establish per second. Default is 1000. Range is 0 to 100000. This option appears only if `type` is `server-loadbalance` and `server-type` is `http`, `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

## portmapping-type {1-to-1 | m-to-n}

The type of port mapping.

- `1-to-1` one-to-one mapping (the default).
- `m-to-n` load balancing (many to many).

This option appears when `type` is not set to `server-load-balance`.

## color <integer>

The color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. To see the colors available, you can edit the VIP from the GUI. 1 is the default color which is black. 0 sets the color to the default color.

## ips

Use `ips` commands to configure IPS sensors to define which signatures are used to examine traffic and what actions are taken when matches are discovered. DoS sensors can also be defined to examine traffic for anomalies.

## ips custom

The IPS sensors use signatures to detect attacks. The FortiGate's predefined signatures cover common attacks. These signatures can be listed with the `config ips rule ?` command. Details about the default settings of each signature can be displayed with the `get` command. If an unusual application or platform is being used, add custom signatures based on the security alerts released by the application and platform vendors. Custom signatures can be used to block or allow specific traffic and provide the power and flexibility to customize FortiGate Intrusion Protection for diverse network environments. You can only edit custom IPS signatures. A single custom signature can be used in multiple sensors with different settings in each.

### Example config ips rule

This example shows how to display the current configuration of the `MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures` signature.

```
config ips rule MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
(MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures) # get
name                : MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
status              : enable
log                 : enable
log-packet          : disable
action              : block
group               : web_client
severity            : high
location            : server, client
os                  : Windows
application         : Other
service             : TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP
rule-id             : 42597
rev                 : 8.928
date                : 1472457600
```

## signature <signature\_str>

The custom signature enclosed in single quotes. For more information, see [Custom IPS Signature Syntax Guide](#).

**severity {all | info | low | medium | high | critical}**

Relative importance of signature, from info to critical. Log messages generated by the signature include the severity.

**location {client | server}**

Specify the type of system to be protected.

**os {all | other | windows | linux | bsd | solaris | macos}**

Operating system(s) that the signature protects. Blank (the default) for all operating systems.

- `all`: all operating systems included.
- `other`: all unlisted operating systems included.

**application [<app1> <app2> ...]**

Application(s) that the signature scans. `set application ?`: lists all applications in the current configuration. Blank (the default) for all applications.

**protocol [<pro1> <pro2> ...]**

Protocol(s) that the signature scans. `set protocol ?`: lists protocols and CLI syntax. Blank (the default) for all protocols

**status {enable | disable}**

Default status of the signature when it is included in an IPS Sensor. Default is `enable`.

**log {enable | disable}**

Enable/disable logging. Default is `enable`.

**log-packet {enable | disable}**

Enable/disable packet logging for this signature. Default is `disable`.

**action {block | pass}**

Default action for this signature. Default is `pass`.

**comment <comment\_str>**

Description of the custom IPS signature. Appears in the profile list. Descriptions with spaces must be enclosed in quotes.

## ips global

This command sets IPS global operating parameters.

### fail-open {enable | disable}

`enable fail-open` ensures that, if IPS should cease to function, crucial network traffic will not be blocked and firewall will continue to operate while the problem is resolved. Default is `disable` which means that if the IPS process fails, IPS traffic is blocked.

### database {regular | extended}

Identify which IPS database to use. Default is `regular`. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.

### traffic-submit {enable | disable}

Enable/disable submission of attack characteristics to FortiGuard Service. Default is `disable`.

### anomaly-mode {continuous | periodical}

Specify blocking mode for rate-based anomaly. Default is `continuous`.

- `continuous` after an anomaly is detected, allow the configured number of packets per second.
- `periodical` block all packets once an anomaly is detected. Overrides individual anomaly settings.

### session-limit-mode {accurate | heuristic}

Select the method that session limit anomalies use to estimate concurrent sessions. Use these options to choose between optimal performance and more accurate information. Default is `heuristic`.

- `accurate` accurately count the concurrent sessions. This option requires more resources than the default heuristics method
- `heuristic` uses heuristics to estimate concurrent sessions. Results may be less accurate but acceptable in most cases.

### intelligent-mode {enable | disable}

Enable/disable IPS adaptive scanning (intelligent mode). Intelligent mode optimizes the scanning method for the type of traffic. Default is `enable`.

### socket-size <ips\_buffer\_size>

Intrusion protection buffer size in MB. Default varies by model depending on available physical memory. Can be changed to tune performance.



## engine-count {integer}

Number of intrusion protection engines to run. Default is 0. Multi-processor FortiGate units can more efficiently process traffic with multiple engines running. When set to the default value of 0, the FortiGate unit determines the optimal number of intrusion protection engines.

## algorithm {engine-pick | low | high | super}

Specify the method used by the IPS engine for determining whether traffic matches signatures. Default is `engine-pick`.

- `engine-pick` allows the IPS engine to choose the best method
- `low` is a slower method that uses less memory
- `high` is a faster method that uses more memory
- `super` is a method that works well on models with more than 4GB memory

## sync-session-ttl {enable | disable}

Enable/disable use of kernel session TTL for IPS sessions. Default is `disable`.

## np-accel-mode {none | basic}

Acceleration mode for IPS processing by NPx processors.

- `none`: NP acceleration disabled.
- `basic`: NP acceleration enabled.

## cp-accel-mode {none | basic | advanced}

CP8 or CP9 acceleration/offloading of pattern matching. For more information see [Hardware Acceleration Overview](#).

- `none` CP8 or CP9 acceleration disabled.
- `basic` offload basic pattern matching to CP8 or CP9 processors.
- `advanced` (the default) offloads more types of pattern matching resulting in higher throughput than basic mode. `advanced` is only available on FortiGate models with two or more CP8s or one or more CP9s.

## skype-client-public-ipaddr <IP\_addr\_list>

Specify the public IP addresses of your network that receive Skype sessions. This will help the FortiGate unit identify Skype sessions properly in the Sessions dashboard widget and when attempting to detect/block them. Separate IP addresses with commas, not spaces.

## deep-app-insp-timeout <seconds>

Sets number of seconds after which inactive application database entries are deleted. Range 1 - 2147483647. Default is 0, and sets recommended value.

## deep-app-insp-db-limit <entries\_int>

Set the maximum number of application database entries. Range: 1 - 2147483647. Default is 0, and sets recommended value.

## exclude-signatures {none | industrial}

Excluded signatures don't appear on the GUI. Used for hiding industrial signatures, which are used by a specialized customer base. Default is `industrial`.

- `none`: no signatures excluded
- `industrial`: exclude industrial signatures

## ips rule

The IPS sensors use signatures to detect attacks. The FortiGate's predefined signatures cover common attacks. These signatures can be listed with the `config ips rule ?` command. Details about the default settings of each signature can be displayed with the `get` command. If an unusual application or platform is being used, add custom signatures based on the security alerts released by the application and platform vendors. Custom signatures can be used to block or allow specific traffic and provide the power and flexibility to customize FortiGate Intrusion Protection for diverse network environments. You can only edit custom IPS signatures. A single custom signature can be used in multiple sensors with different settings in each.

### Example config ips rule

This example shows how to display the current configuration of the `MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures` signature.

```
config ips rule MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
(MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures) # get
name                : MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
status              : enable
log                 : enable
log-packet          : disable
action              : block
group               : web_client
severity            : high
location            : server, client
os                  : Windows
application         : Other
service             : TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP
rule-id             : 42597
rev                 : 8.928
date                : 1472457600
```

## signature <signature\_str>

The custom signature enclosed in single quotes. For more information, see [Custom IPS Signature Syntax Guide](#).

**severity {all | info | low | medium | high | critical}**

Relative importance of signature, from info to critical. Log messages generated by the signature include the severity.

**location {client | server}**

Specify the type of system to be protected.

**os {all | other | windows | linux | bsd | solaris | macos}**

Operating system(s) that the signature protects. Blank (the default) for all operating systems.

- `all`: all operating systems included.
- `other`: all unlisted operating systems included.

**application [<app1> <app2> ...]**

Application(s) that the signature scans. `set application ?`: lists all applications in the current configuration. Blank (the default) for all applications.

**protocol [<pro1> <pro2> ...]**

Protocol(s) that the signature scans. `set protocol ?`: lists protocols and CLI syntax. Blank (the default) for all protocols.

**status {enable | disable}**

Default status of the signature when it is included in an IPS Sensor. Default is `enable`.

**log {enable | disable}**

Enable/disable logging. Default is `enable`.

**log-packet {enable | disable}**

Enable/disable packet logging for this signature. Default is `disable`.

**action {block | pass}**

Default action for this signature. Default is `pass`.

**comment <comment\_str>**

Description of the custom IPS signature. Appears in the profile list. Descriptions with spaces must be enclosed in quotes.

## ips sensor

The IPS sensors use signatures to detect attacks. IPS sensors are made up of filters and override rules. Each filter specifies a number of signature attributes and all signatures matching all the specified attributes are included in the filter.

### comment <comment\_str>

Enter an optional comment to describe the sensor. This description will appear in the IPS sensor list. Descriptions with spaces must be enclosed in quotes.

### replacemsg-group <replacemsg\_str>

Specify the replacement message group.

### block-malicious-url {enable | disable}

Enable/disable blocking of malicious URLs. Default is `disable`.

## config entries

### rule <rule1\_int> [<rule2\_int> <rule3\_int> ...]

Use rule ID to identify the predefined or custom IPS signatures to add to sensor.

### location {all | client | server}

Specify the type of system to be protected. Default is `all`.

### severity {all | info | low | medium | high | critical}

Relative importance of signature, from info to critical. Default is `all`.

### protocol <prot1\_str> [<prot2\_str> <prot3\_str> . . .]

Specify protocols to be examined.

- `?` lists available protocols.
- `all` includes all protocols.
- `other` includes all unlisted protocols

### os {all | other | windows | linux | bsd | solaris | macos}

Specify operating systems to be protected. Default is `all`.

- `all` includes all operating systems.
- `other` includes all unlisted operating systems

## **application <app1\_str> [<app2\_str> <app3\_str> . . .]**

Specify applications to be protected.

- `?` lists available applications.
- `all` includes all applications.
- `other` includes all unlisted applications.

## **tags <tag\_str>**

Assign a custom tag filter to the IPS sensor. Tag must first be configured by using `config system object-tag`. To see what tags are available for use, use the command `set tags ?`. Separate multiple values with a space.

## **status {default | enable | disable}**

Specify status of the signatures included in filter. Default is `default`.

- `default` enables the filter and only use filters with default status of `enable`. Filters with default status of `disable` will not be used.

## **log {default | enable | disable}**

Specify the logging status of the signatures included in the filter. Default is `default`.

- `default` enable logging for only the filters with a default logging status of `enable`. Filters with a default logging status of `disable` will not be logged.

## **log-packet {enable | disable}**

Enable/disable packet logging. `enable` saves the packet that triggers the filter. Default is `disable`.

You can download the packets in pcap format for diagnostic use. This feature is only available in FortiGate units with internal hard drives.

## **log-attack-context {default | enable | disable}**

Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer. Default is `disable`.

## **action {block | default | pass | reject}**

Specify what action is taken with traffic in which signatures are detected. Default is `default`.

- `block` will drop the session with offending traffic.
- `pass` allow the traffic.
- `reject` reset the session.
- `default` either pass or drop matching traffic, depending on the default action of each signature.

## **quarantine {attacker | none}**

Specify how the FortiGate will quarantine attackers. Default is `none`.

- `attacker` blocks all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.

- `none` disables the adding of addresses to the quarantine.

### config exempt-ip

This subcommand is available after rule has been set.

#### edit <exempt-ip\_id>

Enter the ID number of an `exempt-ip` entry. For a list of the `exempt-ip` entries in the IPS sensor, enter ? instead of an ID. Enter a new ID to create a new `exempt-ip`.

#### dst-ip <ip4mask>

Enter destination IP address and netmask to exempt.

#### src-ip <ip4mask>

Enter source IP address and netmask to exempt.

## log

Use the config log commands to set the logging type, the logging severity level, and the logging location for the FortiGate unit.

## log custom-field

Use `log custom-field` to create custom fields that will be included with log messages. **Note:** 'id' will not appear in log messages, it is only used for database purposes.

### edit <id>

A table value for custom fields in log messages. Edit to create new and configure the custom fields using the following entries:

#### name <name>

The name of the field, which will appear in log messages.

#### value <value>

The content of the field, which will appear in log messages.

## log eventfilter

Use `log eventfilter` to select which Event log messages will be recorded.

**Note:** `event` must be enabled for any of the other options to appear. Disabling it overrides all other enabled log types in this category.

### **event {enable | disable}**

Enable or disable logging of all Event logs, which track various FortiGate system and function events.

### **system {enable | disable}**

Enable or disable logging of system activity messages, HA activity messages, CPU & memory usage, VIP realserver health monitoring, and AMC interface bypass mode messages.

### **vpn {enable | disable}**

Enable or disable logging of VPN messages, IPSec negotiation messages, SSL user authentication, administration and session messages.

### **user {enable | disable}**

Enable or disable logging of user authentication events.

### **router {enable | disable}**

Enable or disable logging of router activity and state change events.

### **wireless-activity {enable | disable}**

Enable or disable logging of wireless activity and state change events.

### **wan-opt {enable | disable}**

Enable or disable logging of WAN Optimization activity and state change events.

### **endpoint {enable | disable}**

Enable or disable logging of Endpoint Control activity and state change events.

### **ha {enable | disable}**

Enable or disable logging of all HA activity and state change events.

### **compliance-check {enable | disable}**

Enable or disable logging of all Compliance-related system events.

## log gui-display

Use `log gui-display` to customize which logging content is visible in the GUI.

### resolve-hosts {enable | disable}

If enabled, Log & Report GUI pages will display resolved hostnames using reverse DNS lookup.

### resolve-apps {enable | disable}

If enabled, the FortiGate will search the Internet Service Database to resolve unknown applications in traffic logs.

### fortiview-unscanned-apps {enable | disable}

Determines whether FortiView will display unscanned applications or not.

### fortiview-local-traffic {enable | disable}

Determines whether FortiView will display local traffic logs.

### location {memory | disk | fortianalyzer | fortiguard}

This command allows you to select which location's logs are visible in the GUI:

- `memory`: GUI will display memory logs.
- `disk`: GUI will display disk logs.
- `fortianalyzer`: GUI will display logs from FortiAnalyzer.
- `fortiguard`: GUI will display logs from FortiCloud.

## log threat-weight

Use `log threat-weight` to enable and customize the threat-weight feature, which assigns logs a threat score based on configurable factors.

**Note:** `status` must be enabled for the rest of the options to be available.

### status {enable | disable}

Enable threat-weight calculation in logs.

---

## config level

Use the below subcommands to set the scores for the four levels of threats.



- edit low <value>
  - edit medium <value>
  - edit high <value>
  - edit critical <value>
- 

### **blocked-connection {disable | low | medium | high | critical}**

Set the threat-weight score for blocked-connection errors. `disable` assigns no score.

### **failed-connection {disable | low | medium | high | critical}**

Set the threat-weight score for failed-connection errors. `disable` assigns no score.

### **malware-detected {disable | low | medium | high | critical}**

Set the threat-weight score for malware detection in logs. `disable` assigns no score.

### **url-block-detected {disable | low | medium | high | critical}**

Set the threat-weight score for URL blocking events. `disable` assigns no score.

### **botnet-connection-detected {disable | low | medium | high | critical}**

Set the threat-weight score for botnet connection detections in logs. `disable` assigns no score.

## **config ips**

Use the following subcommands to set the threat score assigned to IPS events at different severity levels:

- set info-severity {disable | low | medium | high | critical}
- set low-severity {disable | low | medium | high | critical}
- set medium-severity {disable | low | medium | high | critical}
- set high-severity {disable | low | medium | high | critical}
- set critical-severity {disable | low | medium | high | critical}

## **config web**

Specific FortiGuard Web Filtering Categories that might appear in logs can be assigned a threat score, using the below commands:

### **edit <id>**

A table value for custom threat score assignments for Categories. Edit to create new and configure the custom assignments using the following commands:

**category <value>**

The Category that will have a threat score assigned to it. You can view a list of Categories by entering `set category ?`.

**level {disable | low | medium | high | critical}**

The threat score assigned to the Web Filtering Category.

## config geolocation

Specific geographic locations that might appear in logs can be assigned a threat score, using the below commands:

**edit <id>**

A table value for custom threat score assignments for countries. Edit to create new and configure the custom assignments using the following commands:

**country <country code>**

The country that will have a threat score assigned to it. You can view a list of country codes by entering `set country ?`.

**level {disable | low | medium | high | critical}**

The threat score assigned to the country.

## config application

Specific FortiGuard Application categories that might appear in logs can be assigned a threat score, using the below commands:

**edit <id>**

A table value for custom threat score assignments for categories. Edit to create new and configure the custom assignments using the following commands:

**category <value>**

The application category that will have a threat score assigned to it. You can view a list of categories by entering `set category ?`.

**level {disable | low | medium | high | critical}**

The threat score assigned to the Application category.

## system

Use system commands to configure options related to the overall operation of your FortiGate.

## system admin

Use this command to add, edit, and delete administrator accounts.

### remote-auth {enable | disable}

Enable or disable authentication of this administrator using a remote RADIUS, LDAP, or TACACS+ server. Disabled by default.

---

### wildcard {enable | disable}

Enable or disable wildcard RADIUS authentication. Disabled by default. This option only appears when `remote-auth` is enabled.

---

### remote-group <name>

Group name used for remote authentication. This option only appears when `remote-auth` is enabled.

---

### password <string>

Set the password for the administrator account.

---

### peer-auth {enable | disable}

Enable or disable peer authentication. Disabled by default.

---

### peer-group <name>

Group name for peer authentication. This option only appears when `peer-auth` is enabled.

---

### {trusthost1 ... trusthost10} <ip\_address>

Set up to ten IPv4 addresses as trusted IPs for authentication.

---

### {ip6-trusthost1 ... ip6-trusthost10} <ip\_address>

Set up to ten IPv6 addresses as trusted IPs for authentication.

---

---

## accprofile <profile-name>

Set the access profile (also known as admin profile) for the account. Access profiles control administrator access to FortiGate features. Two default profiles are available: `prof_admin` and `super_admin`.

---

## accprofile-override {enable | disable}

Enable or disable allowing the remote server to override the administrator's access profile. Disabled by default. This option only appears when `remote-auth` is enabled.

---

## radius-vdom-override {enable | disable}

Enable or disable allowing the remote server to override VDOM access. Only available with wildcard RADIUS authentication. Disabled by default. This option only appears when `remote-auth` is enabled.

---

## allow-remove-admin-session {enable | disable}

Enable or disable allowing session initiated by this administrator to be removed by a privileged administrator. Enabled by default. This field is available for accounts with the `super_admin` profile.

---

## comments <string>

Add comments.

---

## vdom <vdom-name>

Select the virtual domain(s) that the administrator can access.

---

## {ssh-public-key1 | ssh-public-key2 | ssh-public-key3} <key-type> <key-value>

Set up to three SSH public keys.

---

## ssh-certificate <certificate-name>

Set a certificate for PKI authentication of the administrator.

---

## schedule <schedule-name>

Set a schedule for the account.

---

## password-expire

Enter the date and time that this administrator's password expires. Enter zero values for no expiry (this is set by default). Date format is YYYY-MM-DD. Time format is HH:MM:SS. This is available only if `config system password-policy` is enabled.

---

## force-password-change {enable | disable}

Enable or disable requiring this administrator to change password at next login. Disabled by default. Disabling this option does not prevent required password changes due to password policy violation or expiry. This is available only if `config system password-policy` is enabled.

---

## two-factor {enable | disable}

Enable or disable two-factor authentication. Disabled by default.

---

## email-to <email-address>

Set an email address to use for two-factor authentication.

---

## sms-server <server>

Set provider to use to send SMS messages for two-factor authentication. This list of available providers is configured using `config system sms-server`.

---

## sms-phone <phone-number>

Set a phone number to use for two-factor authentication.

---

## guest-auth {enable | disable}

Enable to restrict the admin account to guest account provisioning. Disabled by default.

---

## guest-usergroups <group-name>

Set the user group(s) to be used for guest user accounts created by this administrator account. This option only appears when the account is restricted to guest account provisioning.

---

## guest-lang <language>

Select a language to use for the guest management portal.

## system central-management

Use this command to configure central management for your FortiGate unit. Central management uses a remote location to backup, restore, and monitor the FortiGate unit's configuration. This can be either a FortiManager or the FortiCloud network.

### mode {normal | backup}

Identify central management mode. Default is normal.

- **normal**: manage and configure the connected FortiGate devices from the FortiManager GUI.
- **backup**: backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally.

### type {fortiguard | fortimanager | none}

Specify the type of central management. Setting `type` to `fortiguard` in the CLI is the same as setting it to FortiCloud in the GUI. FortiCloud used to be known as the FortiGuard Analysis and Management Service network. Default is fortimanager.

### schedule-config-restore {enable | disable}

Enable/disable scheduling the restoration of your FortiGate's configuration. Default is enable.

### schedule-script-restore {enable | disable}

Enable/disable scheduling the restoration of your FortiGate's configuration through scripts. Default is enable.

### allow-push-configuration {enable | disable}

Enable/disable configuration image push updates for your FortiGate. Default is enable.

### allow-pushd-firmware {enable | disable}

Enable/disable push firmware. Default is enable.

### allow-remote-firmware-upgrade {enable | disable}

Enable/disable remote upgrading of your FortiGate to a new firmware. Default is enable.

### allow-monitor {enable | disable}

Enable/disable remote monitoring of your FortiGate unit. Default is enable.

**fmg <fmg\_ipv4>**

Specify the IP address or FQDN of the remote FortiManager server. Appears only when `type` is set to `fortimanager`.

**fmg-source-ip <address\_ipv4>**

Specify the source IPv4 address to use when connecting to FortiManager. Appears only when `type` is set to `fortimanager`.

**fmg-source-ip6**

Specify the source IPv6 address to use when connecting to FortiManager. Appears only when `type` is set to `fortimanager`.

**vdom <name\_str>**

Optional. Specify name of virtual domain (VDM) to use when communicating with FortiManager. Default is `root`.

**enc-algorithm {default | high | low}**

Specify encryption strength for communications between the FortiGate unit and FortiManager. Default is `high`.

- `default`: high- and medium-strength algorithms
- `high`: 128-bit and larger key length algorithms
- `low`: 64-bit or 56-bit key length algorithms without export restrictions

**config server-list****server-type {rating | update}**

Specify the FortiGuard service type.

- `rating`: web filter or anti-spam rating server
- `update`: AV, IPS, or AV-query server

**addr-type {ipv4 | ipv6}**

Identify override server's address type.

**server-address <ipv4>**

Specify the override server's IPv4 address.

**server-address6 <ipv6>**

Specify the override server's IPv6 address.

---

## system csf

Configure the network as a Cooperative Security Fabric (CSF)

### status {enable | disable}

Enable or disable the security fabric. The default is `disable`.

---

### upstream-ip <ip-address>

The IP address of the upstream FortiGate.

---

### upstream-port <port-number>

The port used by the upstream FortiGate for communication within the security fabric. The default is `8013`.

---

### group-name <name>

The name of the security fabric.

---

### group-password <password>

The password for the security fabric.

---

### logging mode {default | local}

The location of logs for the fabric. The two options are:

- `default`: Traffic is logged if it has not already been logged by another FortiGate
- `local`: All traffic logging is done according to the FortiGate's local settings

The default is `default`.

---

### management-ip <ip-address>

The management IP address of this FortiGate.



## system dhcp\_server

Configure DHCP servers used to assign IP settings, including IP addresses, to devices connected to a FortiGate interface.

### status {disable | enable}

Enable or disable this DHCP server, default is enable.

---

### lease-time <integer>

Lease time in seconds, value between 300 and 8640000 ( 5 minutes to almost 100 days), 0 for unlimited lease time, default is 604800.

---

### mac-acl-default-action {assign | block}

MAC access control default action. Set whether or not the DHCP server assigns network settings to a DHCP client with a MAC address that is on the MAC address control list.

- `assign` allow the DHCP server to assign IP settings to a client on the MAC address control list.
  - `block` block the DHCP from assigning IP settings to a client on the MAC address control list.
- 

### forticlient-on-net-status {disable | enable}

Enable or disable the FortiClient-On-Net service for this DHCP server, default is enable.

---

### dns-service {local | default | specify}

How the DHCP clients are assigned DNS servers.

- `local` IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.
  - `default` IP addresses of the DNS servers added to the FortiGate configuration become the client's DNS server IP addresses.
  - `specify` specify up to 3 DNS servers in the DHCP server configuration.
- 

### dns-server1 <ip>

Set the IP address of DNS server(s) which will be used by DHCP clients, up to three DNS servers (dns-server1, dns-server2, and dns-server3).

---

---

### wifi-ac1 <ip>

Set the IP address of up to three WiFi Access Controller(s) (wifi-ac1, wifi-ac2, and wifi-ac3). For DHCP option 138 to use DHCP to send WiFi access controller IP addresses to Wireless Termination Points (WTPs) ([RFC 5417](#)).

---

### ntp-service {local | default | specify}

How the DHCP clients are assigned Network Time Protocol (NTP) servers.

- `local` IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.
  - `default` IP addresses of the NTP servers added to the FortiGate configuration become the client's NTP server IP addresses.
  - `specify` specify up to 3 NTP servers in the DHCP server configuration.
- 

### ntp-server1 <ip>

Set the IP address of NTP server(s), up to three NTP servers (ntp-server1, ntp-server2, and ntp-server3).

---

### domain <string>

Domain name suffix for the IP addresses that the DHCP server assigns to clients.

---

### wins-server1 <ip>

Set the IP address of WINS server(s), up to two WINS servers (wins-server1, and wins-server2).

---

### default-gateway <ip>

The default gateway IP address that will be used by DHCP clients as their default gateway.

---

### next-server <ip>

The IP address of the next bootstrap server. Add an IP address if you are using a secondary DHCP server to assign IP configuration options.

---

### netmask <netmask>

The netmask assigned by the DHCP server

---

## interface <interface-name>

The DHCP server can assign IP configurations to DHCP clients connected to this interface.

---

## config ip-range

DHCP IP range configuration.

### start-ip <ip>

The first IP of the range.

### end-ip <ip>

The last IP of the range.

---

## timezone-option {disable | default | specify}

How the DHCP server sets the client's time zone.

- `disable` do not set the client's time zone.
- `default` DHCP clients are assigned the FortiGate's configured time zone.
- `specify` specify the time zone to be assigned to DHCP clients.

## timezone <timezone-number>

Select the time zone that the DHCP server assigns to DHCP clients. Available if `timezone-option` is set to `specify`.

## tftp-server <string>

Hostname or IP address of the TFTP server.

---

## filename <string>

The file name on the tftp server.

---

## config options

The DHCP options configuration.

### code <integer>

The option's code for DHCP, see [RFC 2132](#) for more details.

---

**type {hex | string | ip}**

DHCP option in hexadecimal, string, or IP, default is hex.

**value <string>**

The value is specified as a single octet. Values are available per option, see [RFC 2132](#) for more details.

---

**server-type {regular | ipsec}**

Regular DHCP service or DHCP over IPsec services.

---

**conflicted-ip-timeout <integer>**

The time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused. Value between 60 to 8640000 seconds (1 minute to 100 days), default is 1800.

---

**auto-configuration {disable | enable}**

Disable or enable auto configuration, default is enable.

---

**ddns-update {disable | enable}**

Disable or enable Dynamic DNS update for DHCP, default is disable.

---

**vci-match {disable | enable}**

Disable or enable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI string are served, default is disabled.

**vci-string <strings>**

One or more VCI strings in quotes and separated by spaces.

---

**config exclude-range**

DHCP exclude range configuration.

**start-ip <ip>**

The first IP of the excluded range.

**end-ip <ip>**

The last IP of the excluded range.

---

**config reserved-address**

How the DHCP server assigns IP settings to specific MAC addresses.

**ip <ip>**

The IP address to be reserved for the client with the MAC address. Only valid if `action` is set to `reserved`.

**mac <mac-address>**

MAC address of the client to be configured by the DHCP server according to the action.

**action {assign | block | reserved}**

How the DHCP server configures the client with the reserved MAC address.

- `assign` the DHCP server treats the client with this MAC address like any other client.
- `block` block the DHCP server from assigning IP settings to the client with this MAC address.
- `reserved` assign the reserved IP address to the client with this MAC address.

**description <string>**

Optionally describe the client with this MAC address.

**system dns**

Configure DNS settings used to resolve domain names to IP addresses, so devices connected to a FortiGate interface can use it.

**primary <ip>**

The primary DNS server IP address, default is 208.91.112.53, a FortiGuard server.

---

**secondary <ip>**

The secondary DNS server IP address, default is 208.91.112.52, a FortiGuard server.

---

**domain <string>**

The domain name suffix for the IP addresses of the DNS server.

---

---

**ip6-primary <ipv6>**

The primary DNS server IPv6 address.

---

**ip6-secondary <ipv6>**

The secondary DNS server IPv6 address.

---

**dns-cache-limit <integer>**

The number of records in the DNS cache, value between 0 and 4294967295, default is 5000.

---

**dns-cache-ttl <integer>**

The duration, in seconds, that the DNS cache retains information, value between 60 and 86400, default is 1800.

---

**cache-notfound-responses {disable | enable}**

Disable or enable response from the DNS server when a record is not in cache, default is `disable`.

---

**source-ip <ip>**

The IP address used by DNS server as it's source IP.

**system global**

Use this command to configure global settings that affect FortiGate systems and configurations.

**admin-concurrent {enable | disable}**

Enable/disable to allow concurrent administrator logins. Default is `enable`. Use `policy-auth-concurrent` for firewall authenticated users.

**admin-console-timeout <secs\_int>**

Specify a console login timeout that overrides the `admintimeout` value. Range: 15 - 300 seconds (15 seconds to 5 minutes). Zero value disables the timeout. Default is 0.

### admin-https-banned-cipher {rc4 | low}

Identify banned ciphers for web administration. Default is `rc4 low`. Administrators can now ban the use of specific cipher suites in the CLI for SSL VPN, so that Payment Card Industry Data Security Standard (PCI-DSS) certification can be met.

### admin-https-pki-required {enable | disable}

Specify admin login method. Default is `disable`.

- `enable`: allows admin user to log in by providing a valid certificate if PKI is enabled for HTTPS administrative access.
- `disable`: allows admin users to log in by providing a valid certificate or password.

### admin-https-redirect {enable | disable}

Enable/disable redirection of HTTP administration access to HTTPS. Not available on low-crypto FortiGates. Default is `disable`.

### admin-https-ssl-versions {ssl3 | tlsv1-0 | tlsv1-1 | tlsv1-2}

Specify allowed SSL/TLS versions for web administration. Default is `tlsv1-1 tlsv1-2`.

### admin-lockout-duration <time\_int>

Set the administration account's lockout duration in seconds for the firewall. Repeated failed login attempts will enable the lockout. Use `admin-lockout-threshold` to set the number of failed attempts that will trigger the lockout. Default is `60`.

### admin-lockout-threshold <failed\_int>

Set the number of failed attempts before the account is locked out for the `admin-lockout-duration`. Default is `.`. Default is `3`.

### admin-login-max <int>

Set the maximum number administrators who can be logged in at same time. Range: 1 - 100. Default is `80`.

### admin-maintainer {enable | disable}

Enable/disable hidden maintainer user login. Default is `enable`. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password is "bcpb" followed by the FortiGate unit serial number. You have limited time to complete this login.

### admin-port <port\_number>

Specify the administrative access port for HTTP. Range: 1 - 65535. Default is `80`.

## admin-scp {enable | disable}

Enable/disable allow system configuration download by secure copy protocol (SCP). You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for an administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. Default is `disable`. To backup a VDOM configuration:

```
config global
    set admin-scp enable
end
config vdom
edit <vdom_name>
```

## admin-server-cert {self-sign | <certificate>}

Identify the admin HTTPS server certificate to use. Default is `self-sign`.

## admin-sport <port\_number>

Specify the administrative access port for HTTPS. Range: 1 - 65535. Default is 443.

## admin-ssh-grace-time <time\_int>

Specify the maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating. Range: 10 - 3600 seconds (10 seconds to one hour). Default is 120.

## admin-ssh-password {enable | disable}

Enable/disable password authentication for SSH admin access. Default is `enable`.

## admin-ssh-port <port\_number>

Specify the administrative access port for SSH. Range: 1 - 65535. Default is 22.

## admin-ssh-v1 {enable | disable}

Enable/disable Secure Shell (SSH) version 1 compatibility. Default is `disable`.

## admin-telnet-port <port\_number>

Specify the administrative access port for TELNET. Range: 1 - 65535. Default is 23.

## admintimeout <admin\_timeout\_minutes>

Specify the number of minutes before an idle administrator times out. The maximum `admintimeout` interval is 480 minutes (8 hours). Default is 5. To improve security keep the idle timeout at the default value.



## alias <alias\_str>

Identify an alias for your FortiGate unit.

## allow-traffic-redirect {enable | disable}

Enable/ disable allow traffic redirect. Default is `enable`. Under some conditions, it is undesirable to have traffic routed back on the same interface. In that case, set `allow-traffic-redirect` to `disable`.

## anti-replay {disable | loose | strict}

Specify the level of checking for packet replay and TCP sequence checking (or TCP Sequence number checking). Default is `strict`. FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets.

- `disable`: no anti-replay protection.
- `loose`: perform packet sequence checking and ICMP anti-replay checking with the following criteria:
  - the SYN, FIN, and RST bit can not appear in the same packet.
  - the FortiGate unit does not allow more than 1 ICMP error packet to go through the FortiGate unit before it receives a normal TCP or UDP packet.
  - If the FortiGate unit receives an RST packet, and `check-reset-range` is set to `strict` the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
- `strict`: performs all of the loose checking but for each new session also checks to determine if the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding.

If any packet fails a check it is dropped. If `loginvalid-packet` is set to `enable`, a log message is written for each packet that fails a check.

## arp-max-entry <int>

Specify the maximum number of dynamically learned MAC addresses that can be added to the ARP table.

Range: 131072 - 2147483647. If set to 0, kernel holds 131072 entries. Default is 0.

## auth-cert <cert-name>

Identify the HTTPS server certificate for policy authentication. Default is `self-sign`. Self-sign is the built-in certificate but others will be listed as you add them.

## auth-http-port <http\_port>

Set the HTTP authentication port. Range: 1 - 65535. Default is 1000.

### auth-https-port <https\_port>

Set the HTTPS authentication port. Range: 1 - 65535. Default is 1003.

### auth-keepalive {enable | disable}

Enable to extend the session's authentication time to prevent an idle timeout. Default is `disable`.

### auto-auth-extension-device {enable | disable}

Enable/disable automatic authorization of dedicated Fortinet extension device globally. Default is `enable`.

### av-affinity <string>

Specify the CPU affinity setting for AV scanning (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx). Setting CPU affinity, where a process will execute on a specific CPU, can be used to conserve resources. Default is 0.

### av-failopen {idledrop | off | one-shot | pass}

Set the action to take if the unit is running low on memory or the proxy connection limit has been reached. Default is `pass`.

- `idledrop`: drop connections based on the clients that have the most connections open. This is most useful for Windows applications, and can prevent malicious bots from keeping an idle connection open to a remote server.
- `off`: stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.
- `one-shot`: bypass the antivirus system when memory is low. You must enter `off` or `pass` to restart antivirus scanning.
- `pass`: bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved

### av-failopen-session {enable | disable}

When enabled and a protocol's proxy runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by `av-failopen`. Default is `disable`.

### batch-cmdb {enable | disable}

Enable/disable batch mode to execute in CMDB server. Batch mode is used to enter a series of commands that will execute as a group once they are loaded. Default is `enable`.

### block-session-timer <int>

Set the time duration in seconds for blocked sessions. Range: 1 - 300 seconds (1 second to 5 minutes). Default is 30.

### br-fdb-max-entry <int>

Specify the maximum number of bridge forwarding database (FDB) entries. Used when operating in Transparent mode, the FDB (or MAC) table is used by a Layer 2 device (switch/bridge) to store MAC addresses that have been learned and the ports that each MAC address was learned on. If the FDB has a large number of entries, performance may be impacted. Range: 8192 - 2147483647. If set to 0, kernel holds 8192 entries. Default is 0.

### cert-chain-max <int>

Set the maximum number of certificates that can be traversed in a certificate chain. The list of certificates, from the root certificate to the end-user certificate, represents the certificate chain. Default is 8.

### cfg-save {automatic | manual | revert}

Specify the configuration file save mode for changes made using the CLI. Default is `automatic`.

- `automatic`: automatically save the configuration after every change.
- `manual`: manually save the configuration using the `execute cfg save` command.
- `revert`: manually save the current configuration and then revert to that saved configuration after `cfg-revert-timeout` expires.

Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode. [/expand]

### check-protocol-header {loose | strict}

Select the level of checking performed on protocol headers. Default is `loose`.

- `loose`: the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc.
- `strict`: the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length. Note: this setting disables hardware acceleration.

If the packet fails header checking it is dropped by the FortiGate unit and logged if `log-invalid-packet` is enabled.

### check-reset-range {disable | strict}

Configure ICMP error message verification. Default is `disable`.

- `disable`: the FortiGate unit does not validate ICMP error messages.
- `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) |TCP(C,D) header and if FortiOS can locate the A:C->B:D session, it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range, then the ICMP packet is dropped. If `log-invalid-packet` is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets

**cli-audit-log {enable | disable}**

Enable/disable CLI audit log. Default is disable.

**clt-cert-req {enable | disable}**

Enable/disable requirement for a client certificate before administrator logs in via GUI using HTTPS. Default is disable.

**compliance-check {enable | disable}**

Enable/disable global PCI DSS compliance check. Default is enable.

**compliance-check-time <HH:MM:SS>**

Specify the PCI DSS compliance check time. Default is 00:00:00.

**csr-ca-attribute {enable | disable}**

Enable/disable the use of CA attribute in your certificate. Some CA servers reject CSRs that have the CA attribute. Default is enable.

**daily restart {enable | disable}**

Enable/disable daily restart of FortiGate unit. Default is disable. The time of the restart is controlled by `restart-time`.

**device-identification-active-scan-delay <int>**

Indicate how many seconds to passively scan a device before performing an active scan. Range: 20 - 3600 seconds (20 seconds to 1 hour). Default is 90.

**device-idle-timeout <int>**

Specify time in seconds that a device must be idle in order to automatically log user out. Range: 30 - 31536000 seconds (30 seconds to 1 year). Default is 300.

**dh-params {1024 | 1536 | 2048 | 3072 | 4096 | 6144 | 8192}**

Minimum size, in bits, of the prime number used in Diffie-Hellman key exchange for HTTPS/SSH protocols. Default is 2048.

**disk-usage {log | wanopt}**

Specify whether to use hard disk or WAN Optimization for logging. Default is log.

**dst {enable | disable}**

Enable/disable daylight saving time. Default is enable.

**endpoint-control-fds-access {enable | disable}**

Enable/disable access to FortiGuard network for non-compliant endpoints. Default is enable.

**endpoint-control-portal-port**

Specify the endpoint control portal port. Range: 1 - 65535. Default is 8009.

**explicit-proxy-auth-timeout <int>**

Specify authentication timeout in seconds for idle sessions in explicit web proxy. Default is 300.

**fds-statistics {enable | disable}**

Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. Default is enable.

**fds-statistics-period <int>**

Indicate the FortiGuard statistics update period in minutes. Range: 1 - 1440 minutes (1 minute to 24 hours). Default is 60.

**fgd-alert-subscription {advisory | latest-threat | latest-virus | latest-attack | new-antivirus-db | new-attack-db}**

Specify the type of alert to retrieve from FortiGuard.

- **advisory:** retrieves FortiGuard advisories, report, and news alerts.
- **latest-threat:** retrieves latest FortiGuard threat alerts.
- **latest-virus:** retrieves latest FortiGuard virus alerts.
- **latest-attack:** retrieves latest FortiGuard attack alerts.
- **new-antivirus-db:** retrieves latest FortiGuard antivirus database release alerts.
- **new attack-db:** retrieves latest FortiGuard IPS database release alerts.

**fortiextender {enable | disable}**

Enable/disable FortiExtender controller. Default is disable.

**fortiextender-data-port <port\_int>**

Specify Fortiextender controller data port. Range: 1024 - 49150. Default is 25246.

### **fortiservice-port <port\_int>**

Specify the FortiService port number. Default is 8013. Starting with FortiClient 5.4, endpoint compliance (EC) registration will use port 8013 by default. To register to FortiOS 5.0 or 5.2, the user must specify port 8010 with the IP address, separated by a colon. For example, <IP\_Address>:8010. FortiOS 5.4 will listen on port 8013. If registering from FortiClient 5.4 to FortiOS 5.4, the default ports will match. Specifying the port number with the IP address is then optional. For more information, refer to [FortiClient 5.4.0 Release Notes](#) which is available in the [Fortinet Document Library](#).

### **gui-certificates {enable | disable}**

Enable/disable certificate configuration in GUI. Default is enable.

### **gui-custom-language {enable | disable}**

Enable/disable custom languages in GUI. Default is disable.

### **gui-device-latitude <string>**

Identify the latitude coordinate of your FortiGate.

### **gui-device-longitude <string>**

Identify the longitude coordinate of your FortiGate.

### **gui-display-hostname {enable | disable}**

Enable/disable display of hostname on GUI login page. Default is disable.

### **gui-ipv6 {enable | disable}**

Enable/disable IPv6 settings in GUI. Default is disable.

### **gui-lines-per-page <gui\_lines>**

Specify number of lines to display per page for web administration. Default is 50.

### **gui-theme {green | red | blue | melongene | mariner}**

Select color scheme to use for the administration GUI. Default is green.

### **gui-wireless-opensecurity {enable | disable}**

Enable/disable wireless open security option in GUI. Default is disable.

### **honor-df {enable | disable}**

Enable/disable honoring of Don't-Fragment (DF) flag. The DF flag instructs routers that would normally fragment a packet that is too large for a link's MTU (and potentially deliver it out of order due to that fragmentation) to instead drop the packet and return an ICMP Fragmentation Needed packet, allowing the sending host to account for the lower MTU on the path to the destination host. Default is enable.

### **hostname <unithostname>**

Specify FortiGate unit hostname. Default is FortiGate serial number.

A hostname can only include letters, numbers, hyphens, and underlines. No spaces allowed.

While the hostname can be longer than 24 characters, if it is longer than 24 characters it will be truncated by a "~". The trailing 3-characters preceded by the "~" truncation character and the first N-3 characters are shown. This shortened hostname will be displayed in the CLI, and other locations the hostname is used. Some models support hostnames up to 35 characters

### **ip-src-port-range <start\_port>-<end\_port>**

Specify the IP source port range used for traffic originating from the FortiGate unit. Range: 1-65535. Default is 1024-499. You can use this setting to avoid problems with networks that block some ports, such as FDN ports.

### **ips-affinity <string>**

Affinity setting for IPS (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).

### **ipsec-asic-offload {enable | disable}**

Enable/disable application-specific integrated circuit (ASIC) offload for IPsec VPN. You can use this command to disable using ASIC offloading to accelerate IPsec Diffie-Hellman key exchange for IPsec ESP traffic. By default hardware offloading is used. For debugging purposes or other reasons you may want this function to be processed by software. Default is enable.

### **ipsec-hmac-offload {disable | enable}**

Enable/disable offload keyed-hashing for message authentication (HMAC) to hardware for IPsec VPN. Default is enable.

### **ipv6-accept-dad {0 | 1 | 2}**

Enable/disable acceptance of IPv6 DAD (Duplicate Address Detection). 0: Disable DAD; 1: Enable DAD (default); 2: Enable DAD, and disable IPv6 operation if MAC-based duplicate link-local address has been found.

## language <string>

Identify the GUI display language. `set language ?` lists available languages. `trach` = Traditional Chinese. `simch` = Simplified Chinese. Default is English.

## ldapconntimeout <integer>

LDAP connection time-out in milliseconds. Range: 0 - 4294967295.

## lldp-transmission {enable | disable}

Enable/disable Link Layer Discovery Protocol (LLDP) transmission. Default is disable.

## log-uuid {disable | policy-only | extended}

Universally Unique Identifier (UUID) log option. Default is policy-only.

## login-timestamp {enable | disable}

Enable/disable login time recording. Default is disable.

## management-vdom <domain>

Management virtual domain name. Default is root.

## max-route-cache-size <int>

Specify the maximum number of IP route cache entries. Range: 0 - 2 147483647. Default is 0.

## miglog-affinity

Affinity setting for logging (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx).

## miglogd-children <int>

Specify the number of miglogd processes to run. A higher number can affect performance, and a lower number can affect log processing time, although no logs will be dropped or lost if the number is decreased. If you are suffering from performance issues, you can alter the number of logging daemon child processes. Range: 0 - 15. Default is 0.

## ndp-max-entry <int>

Specify the maximum number of Neighbor Discovery Protocol (NDP) table entries. Set to 65,536 or higher; if set to 0, kernel holds 65,536 entries. Default is 0. Specify the maximum number of Neighbor Discovery Protocol (NDP) table entries. Set to 65,536 or higher; if set to 0, kernel holds 65,536 entries. Default is 0.



**optimize {antivirus}**

DO NOT USE THIS COMMAND. It was originally added to early NP4 platforms but is no longer supported.

**phase1-rekey {enable | disable}**

Enable/disable rekeying between Internet Key Exchange (IKE) peers before the phase 1 keylife expires. Default is enable.

**policy-auth-concurrent <limit\_int>**

Limit the number of concurrent logins from the same user. Range: 1 - 100. Default is 0 and means no limit.

**post-login-banner {enable | disable}**

Enable/disable to display the admin access disclaimer message after successful login. Default is disable.

**pre-login-banner {enable | disable}**

Enable/disable to display the admin access disclaimer prior to login. Default is disable.

**private-data-encryption {enable | disable}**

Enable/disable private data encryption using an AES 128-bit key. Default is disable.

**proxy-cipher-hardware-acceleration {enable | disable}**

Enable/disable use of content processor to encrypt or decrypt traffic. Default is enable.

**proxy-kxp-hardware-acceleration {enable | disable}**

Enable/disable use of content processor to encrypt or decrypt traffic. Default is enable.

**proxy-worker-count <count\_int>**

Specify the number of proxy worker processes. Range: 1 - 8. Default is 4.

**radius-port <radius\_port>**

Specify the port for RADIUS traffic. Default is 1812. If your RADIUS server is using port 1645, you can use the CLI to change the RADIUS port on your FortiGate unit.

**reboot-upon-config-restore {enable | disable}**

Enable/disable reboot of system when restoring configuration. Default is enable.

## refresh <refresh\_seconds>

Specify the Automatic Refresh Interval, in seconds, for GUI statistics. Range: 0-4294967295. Default is 0, or no automatic refresh.

## registration-notification {enable | disable}

Enable/disable displaying the registration notification if the FortiGate is not registered. Default is enable.

## remoteauthtimeout <timeout\_sec>

Specify the number of seconds that the FortiGate unit waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. Range: 0-300 seconds, 0 means no timeout. Default is 5. To improve security keep the remote authentication timeout at the default value of 5 seconds. However, if a RADIUS request needs to traverse multiple hops or several RADIUS requests are made, the default timeout of 5 seconds may not be long enough to receive a response.

## reset-sessionless-tcp {enable | disable}

The `reset-sessionless-tcp` command determines what action the FortiGate unit performs if it receives a TCP packet but cannot find a corresponding session in its session table. This happens most often because the session has timed out. In most cases you should leave `reset-sessionless-tcp` set to disable (the default). When this command is set to disable, the FortiGate unit silently drops the packet. The packet originator does not know that the session has expired and might re-transmit the packet several times before attempting to start a new session. Enabling this option may help resolve issues with a problematic server, but it can make the FortiGate unit more vulnerable to denial of service attacks. If you enable `reset-sessionless-tcp`, the FortiGate unit sends a RESET packet to the packet originator. The packet originator ends the current session, but it can try to establish a new session. Available in NAT/Route mode only. Default is disable.

## revision-backup-on-logout {enable | disable}

Enable/disable back-up of the latest configuration revision when the administrator logs out of the CLI or GUI. Default is disable.

## revision-image-auto-backup {enable | disable}

Enable/disable back-up of the latest configuration revision when firmware is upgraded. Default is disable.

## scanunit-count <count\_int>

Tune the number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs. Recommended for advanced users.

**send-pmtu-icmp {enable | disable}**

Enable to send a path maximum transmission unit (PMTU) - ICMP destination unreachable packet and to support PMTUD protocol on your network to reduce fragmentation of packets. Disabling this command will result in PMTUD packets being blocked. Default is enable.

**service-expire-notification {enable | disable}**

Enable/disable display of a 30-day notice of support contract expiry on GUI. Default is enable.

**snat-route-change {enable | disable}**

Enable/disable static NAT route change. Default is disable.

**special-file-23-support {enable | disable}**

Enable/disable IPS detection of HIBUN format files when using Data Leak Protection. Default is disable.

**sslvpn-cipher-hardware-acceleration {enable | disable}**

Enable/disable SSL VPN hardware acceleration.

**sslvpn-kxp-hardware-acceleration {enable | disable}**

Enable/disable SSL VPN KXP hardware acceleration.

**sslvpn-max-worker-count <count\_int>**

Specify the maximum number of SSL VPN processes. The upper limit for setting this value is the number of CPUs and depends on the model.

**sslvpn-plugin-version-check {enable | disable}**

Enable/disable checking browser's plugin version. Default is enable.

**strict-dirty-session-check {enable | disable}**

Enable to check the session against the original policy when revalidating. This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together. If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session. Default is enable.

**strong-crypto {enable | disable}**

Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). In addition, some low-crypto options are not available. Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption. Default is

disable. Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). In addition, some low-crypto options are not available. Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption. Default is disable.

### switch-controller {enable | disable}

Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself. Default is disable.

### switch-controller-reserved-network <ipv4mask>

Enable reserved network subnet for controlled switches. This is available when the switch controller is enabled. Default: 169.254.0.0 255.255.0.0

### syncinterval <ntpsync\_minutes>

Specify how often, in minutes, the FortiGate unit should synchronize its time with the Network Time Protocol (NTP) server. Range: 1 - 1440 minutes (1 day). Setting to 0 disables time synchronization. Default is 0.

### sys-perf-log-interval <int>

Set the time in minutes between updates of performance statistics logging. Range: 1 - 15 minutes. 0 disables performance logging. Default is 5.

### tcp-halfclose-timer <seconds>

Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. Range: 1 - 86400 seconds (1 day). Default is 120.

### tcp-halfopen-timer <seconds>

Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. Range: 1 - 86400 seconds (1 day). Default is 10.

### tcp-option {enable | disable}

Enable SACK, timestamp and MSS TCP options. For normal operation, `tcp-option` should be enabled. Disable for performance testing or, in rare cases, where it impairs performance. Default is enable.

### tcp-timewait-timer <seconds\_int>

Set the length of the TCP TIME-WAIT state in seconds. As described in [RFC 793](#), the "TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request". Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. Range: 0 - 300 seconds. Default is 1.

## timezone <timezone\_number>

The number corresponding to your time zone from 00 to 86. Enter `set timezone ?` to view the list of time zones and the numbers that represent them. Default is 00, which is equivalent to GMT +12.

## tp-mc-skip-policy {enable | disable}

Enable to allow skipping of the policy check, and to enable multicast traffic through. Default is disable. Multicasting (also called IP multicasting) is a technique for one-to-many and many-to-many real-time communication over an IP infrastructure in a network. Multicast uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. can be used to send data to many receivers simultaneously while conserving bandwidth and reducing network traffic. Multicasting can be used for one-way delivery of media streams to multiple receivers and for one-way data transmission for news feeds, financial information, and so on.

## traffic-priority {tos | dscp}

Select Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping. Default is tos. For more information, see the Handbook's discussion of [ToS and DSCP traffic mapping](#).

## traffic-priority-level {low | medium | high}

Select the default system-wide level of priority for traffic prioritization. This determines the priority of traffic for scheduling, typically set on a per service type level. For more information, see `system tos-based-priority` or `system dscp-based-priority` or the [Traffic Shaping](#) chapter in the Handbook. Default is medium.

## two-factor-email-expiry <seconds\_int>

Set the timeout period for email-based two-factor authentication. Two-factor email authentication sends a randomly generated six-digit numeric code to a specified email address. The recipient must enter that code when prompted and that code is only valid for the time period set by this command. Range: 30 - 300 seconds (5 minutes). Default is 60.

## two-factor-fac-expiry <seconds\_int>

Set the timeout period for FortiAuthenticator token authentication. A FortiAuthenticator provides RADIUS, LDAP and 802.1X wireless authentication, certificate management, and Fortinet Single Sign-on (FSSO). FortiAuthenticator is compatible with FortiToken to provide two-factor authentication with multiple FortiGates and third party devices. Range: 10 - 3600 seconds (1 hour). Default is 60.

## two-factor-ftk-expiry <seconds\_int>

Set the timeout period for FortiToken authentication. Range: 60 - 600 seconds (10 minutes). Default is 60. FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes at the end of the timeout period set by this command.

## two-factor-ftm-expiry <hours\_int>

Set the timeout period for FortiToken Mobile provision. Range: 1 - 168 hours (7 days). Default is 72. FortiToken Mobile performs much the same function as the FortiToken except the physical device is replaced by a mobile phone application and the timeout period is set in hours, not seconds.

## two-factor-sms-expiry <seconds\_int>

Set the timeout period for SMS-based two-factor authentication. Range 30 - 300 seconds. Default is 60. SMS two-factor authentication sends the token code in an SMS text message to the mobile device indicated when this user attempts to logon. This token code is valid only for the time period set by this command. SMS two-factor authentication has the benefit of not requiring email service before logging on. A potential issue is if the mobile service provider does not send the SMS text message before the life of the token expires.

## udp-idle-timer <seconds>

Enter the number of seconds before an idle UDP connection times out. This command can be useful in managing unit CPU and memory resources. Range: 1 - 86400 seconds (1 day). Default is 180.

## user-server-cert <cert\_name>

Select the certificate to use for https user authentication. Default setting is `Fortinet_Factory`, if available, otherwise `self-sign`.

## vdom-admin {enable | disable}

Enable/disable configuration of multiple virtual domains. Default is disable.

## vip-arp-range {restricted |unlimited}

`vip-arp-range` controls the number of Address Resolution Protocol (ARP) packets the FortiGate unit sends for a Virtual IP (VIP) address range. Default is restricted.

- `restricted`: the FortiGate unit sends ARP packets for only the first 8192 addresses in a VIP range.
- `unlimited`: the FortiGate unit sends ARP packets for every address in the VIP range.

## virtual-server-count <integer>

Enter the number of virtual server processes to create. The maximum is the number of CPU cores. This is not available on single-core CPUs.

## virtual-server-hardware-acceleration {enable | disable}

Enable/disable virtual server hardware acceleration. Default is enable.

### wad-worker-count <int>

Set the number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy and web caching is handled by half of the CPU cores in a FortiGate unit. For example, if your FortiGate unit has 4 CPU cores, by default two will be used for WAN optimization, explicit proxy and web caching. You can use the `wad-worker-count` command to change the number of CPU cores that are used. Range: 1 to the number of CPU cores.

### wifi-ca-certificate <ca\_cert-name>

Select the CA certificate that verifies the WiFi certificate.

### wifi-certificate <cert-name>

Select the certificate to use for WiFi authentication.

### wimax-4g-usb {enable | disable}

Enable/disable access to a Worldwide Interoperability for Microwave Access (WiMAX) 4G USB device. FortiGate units support the use of wireless, 3G and 4G modems connected using the USB port or, if available, the express card slot. Modem access provides either primary or secondary (redundant) access to the Internet. For FortiGate units that do not include an internal modem (those units with an "M" designation), the modem interface will not appear in the web-based manager until enabled in the CLI. Default is disable.

### wireless-controller {enable | disable}

Enable/disable the wireless (WiFi) daemon. Default is enable.

### wireless-controller-port <port\_int>

Select the port used for the control channel in wireless controller mode (`wireless-mode is ac`). The data channel port is the control channel port number plus one. Range: 1024 - 49150. Default is 5246.

## system ha

Enable and configure FortiGate FGCP high availability (HA) and virtual clustering. Some of these options are also used for FGSP HA and content clustering.



In FGCP HA mode, most settings are automatically synchronized among cluster units. The following settings are not synchronized:

- override
- priority (including the secondary-vcluster priority)
- ha-mgmt-interface-gateway
- ha-mgmt-interface-gateway6
- cpu-threshold, memory-threshold, http-proxy-threshold, ftp-proxy-threshold, imap-proxy-threshold, nntp-proxy-threshold, pop3-proxy-threshold, smtp-proxy-threshold
- The ha-priority setting of the config system link-monitor command
- The config system interface settings of the FortiGate interface that becomes an HA reserved management interface
- The config system global hostname setting.

### group-id <id>

The HA group ID, same for all members, from 0 to 255. The group ID identifies individual clusters on the network because the group ID affects the cluster virtual MAC address. All cluster members must have the same group ID. If you have more than two clusters on the same network they must have different Group IDs.

### group-name <name>

The HA group name, same for all members. Max 32 characters. The HA group name identifies the cluster. All cluster members must have the same group name. Can be blank if `mode` is `standalone`.

### mode {standalone | a-a | a-p}

The HA mode.

- `standalone` to disable HA. The mode required for FGSP.
- `a-a` to create an Active-Active cluster.
- `a-p` to create an Active-Passive cluster.

All members of an HA cluster must be set to the same HA mode.

### password <password>

The HA cluster password, must be the same for all cluster units. The maximum password length is 15 characters.

### hbdev <interface-name> <priority> [<interface-name> <priority>]...

Select the FortiGate interfaces to be heartbeat interfaces and set the heartbeat priority for each interface. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface that with the lowest hash map order value processes all heartbeat traffic.

By default two interfaces are configured to be heartbeat interfaces and the priority for both these interfaces is set to 50. The heartbeat interface priority range is 0 to 512.



You can select up to 8 heartbeat interfaces. This limit only applies to FortiGate units with more than 8 physical interfaces.

You can use the `append` command to add more entries. The default depends on the FortiGate model.

### **session-sync-dev <interface>**

Select one or more FortiGate interfaces to use for synchronizing sessions as required for session pickup. Normally session synchronization occurs over the HA heartbeat link. Using this HA option means only the selected interfaces are used for session synchronization and not the HA heartbeat link. If you select more than one interface, session synchronization traffic is load balanced among the selected interfaces.

Moving session synchronization from the HA heartbeat interface reduces the bandwidth required for HA heartbeat traffic and may improve the efficiency and performance of the cluster, especially if the cluster is synchronizing a large number of sessions. Load balancing session synchronization among multiple interfaces can further improve performance and efficiency if the cluster is synchronizing a large number of sessions.

Session synchronization packets use Ethertype 0x8892. The interfaces to use for session synchronization must be connected together either directly using the appropriate cable (possible if there are only two units in the cluster) or using switches. If one of the interfaces becomes disconnected the cluster uses the remaining interfaces for session synchronization. If all of the session synchronization interfaces become disconnected, session synchronization reverts back to using the HA heartbeat link. All session synchronization traffic is between the primary unit and each subordinate unit.

Since large amounts of session synchronization traffic can increase network congestion, it is recommended that you keep this traffic off of your network by using dedicated connections for it.

### **route-ttl <ttl>**

Control how long routes remain in a cluster unit's routing table. The time to live range is 5 to 3600 seconds (3600 seconds is one hour). The default time to live is 10 seconds.

The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. To maintain communication sessions after a cluster unit becomes a primary unit, routes remain active in the routing table for the route time to live while the new primary unit acquires new routes.

By default, `route-ttl` is set to 10 which may mean that only a few routes will remain in the routing table after a failover. Normally keeping `route-ttl` to 10 or reducing the value to 5 is acceptable because acquiring new routes usually occurs very quickly, especially if graceful restart is enabled, so only a minor delay is caused by acquiring new routes.

If the primary unit needs to acquire a very large number of routes, or if for other reasons there is a delay in acquiring all routes, the primary unit may not be able to maintain all communication sessions.

You can increase the route time to live if you find that communication sessions are lost after a failover so that the primary unit can use synchronized routes that are already in the routing table, instead of waiting to acquire new routes.

### **route-wait <wait>**

The amount of time in seconds that the primary unit waits after receiving routing updates before sending the updates to the subordinate units. For quick routing table updates to occur, set `route-wait` to a relatively short

time so that the primary unit does not hold routing table changes for too long before updating the subordinate units.

The `route-wait` range is 0 to 3600 seconds. The default `route-wait` is 0 seconds. Normally, because the is 0 seconds.

Normally, because the `route-wait` time is 0 seconds the primary unit sends routing table updates to the subordinate units every time its routing table changes.

Once a routing table update is sent, the primary unit waits the `route-hold` time before sending the next update.

Usually routing table updates are periodic and sporadic. Subordinate units should receive these changes as soon as possible so `route-wait` is set to 0 seconds. `route-hold` can be set to a relatively long time because normally the next route update would not occur for a while.

In some cases, routing table updates can occur in bursts. A large burst of routing table updates can occur if a router or a link on a network fails or changes. When a burst of routing table updates occurs, there is a potential that the primary unit could flood the subordinate units with routing table updates. Flooding routing table updates can affect cluster performance if a great deal of routing information is synchronized between cluster units. Setting `route-wait` to a longer time reduces the frequency of additional updates and prevents flooding of routing table updates from occurring.

### **route-hold <hold>**

The amount of time in seconds that the primary unit waits between sending routing table updates to subordinate units. The route hold range is 0 to 3600 seconds. The default route hold time is 10 seconds.

To avoid flooding routing table updates to subordinate units, set `route-hold` to a relatively long time to prevent subsequent updates from occurring too quickly. Flooding routing table updates can affect cluster performance if a great deal of routing information is synchronized between cluster units. Increasing the time between updates means that this data exchange will not have to happen so often.

The `route-hold` time should be coordinated with the `route-wait` time.

### **sync-config {disable | enable}**

Enable or disable automatic synchronization configuration changes to all cluster units.

### **encryption {disable | enable}**

Enable or disable HA heartbeat message encryption using AES-128 for encryption and SHA1 for authentication. Disabled by default.

### **authentication {disable | enable}**

Enable or disable HA heartbeat message authentication using SHA1. Disabled by default.

### **hb-interval <interval>**

The time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100\*milliseconds). The default is 2.

A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms ( $5 * 100\text{ms} = 500\text{ms}$ ).

HA heartbeat packets consume more bandwidth if the heartbeat interval is short. But if the heartbeat interval is very long, the cluster is not as sensitive to topology and other network changes.

The heartbeat interval combines with the lost heartbeat threshold to set how long a cluster unit waits before assuming that another cluster unit has failed and is no longer sending heartbeat packets. By default, if a cluster unit does not receive a heartbeat packet from a cluster unit for  $6 * 200 = 1200$  milliseconds or 1.2 seconds the cluster unit assumes that the other cluster unit has failed.

You can increase both the heartbeat interval and the lost heartbeat threshold to reduce false positives. For example, increasing the heartbeat interval to 20 and the lost heartbeat threshold to 30 means a failure will be assumed if no heartbeat packets are received after  $30 * 2000$  milliseconds = 60,000 milliseconds, or 60 seconds.

### **hb-lost-threshold <threshold>**

The number of consecutive heartbeat packets that are not received from another cluster unit before assuming that the cluster unit has failed. The default value is 6, meaning that if the 6 heartbeat packets are not received from a cluster unit then that cluster unit is considered to have failed. The range is 1 to 60 packets.

If the primary unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed.

If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit.

The lower the `hb-lost-threshold` the faster a cluster responds when a unit fails. However, sometimes heartbeat packets may not be sent because a cluster unit is very busy. This can lead to a false positive failure detection. To reduce these false positives you can increase the `hb-lost-threshold`.

### **hello-holddown <timer>**

The number of seconds that a cluster unit waits before changing from the hello state to the work state. The default is 20 seconds and the range is 5 to 300 seconds.

The hello state hold-down time is the number of seconds that a cluster unit waits before changing from hello state to work state. After a failure or when starting up, cluster units operate in the hello state to send and receive heartbeat packets so that all the cluster units can find each other and form a cluster. A cluster unit should change from the hello state to work state after it finds all of the other FortiGate units to form a cluster with. If for some reason all cluster units cannot find each other during the hello state then some cluster units may be joining the cluster after it has formed. This can cause disruptions to the cluster and affect how it operates.

One reason for a delay in all of the cluster units joining the cluster could be the cluster units are located at different sites or if for some other reason communication is delayed between the heartbeat interfaces.

If cluster units are joining your cluster after it has started up or if it takes a while for units to join the cluster you can increase the time that the cluster units wait in the hello state.

### **gratuitous-arps {disable | enable}**

Enable or disable sending gratuitous ARP packets from a new master unit. Enabled by default.

In most cases you would want to send gratuitous ARP packets because its a reliable way for the cluster to notify the network to send traffic to the new primary unit. However, in some cases, sending gratuitous ARP packets may be less optimal. For example, if you have a cluster of FortiGate units in Transparent mode, after a failover the new primary unit will send gratuitous ARP packets to all of the addresses in its Forwarding Database (FDB). If the FDB has a large number of addresses it may take extra time to send all the packets and the sudden burst of traffic could disrupt the network.

If you choose to disable sending gratuitous ARP packets you must first enable the `link-failed-signal` setting. The cluster must have some way of informing attached network devices that a failover has occurred.

## arps <number>

The number of times that the primary unit sends gratuitous ARP packets. Gratuitous ARP packets are sent when a cluster unit becomes a primary unit (this can occur when the cluster is starting up or after a failover). The default is 5 packets, the range is 1 to 60.

Usually you would not change the default setting of 5. In some cases, however, you might want to reduce the number of gratuitous ARP packets. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending a higher number gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully, you could reduce the number of gratuitous ARP packets that are sent to reduce the amount of traffic produced after a failover.

If failover is taking longer than expected, you may be able to reduce the failover time by increasing the number of gratuitous ARP packets sent.

## arps-interval <interval>

The number of seconds to wait between sending gratuitous ARP packets. When a cluster unit becomes a primary unit (this occurs when the cluster is starting up or after a failover) the primary unit sends gratuitous ARP packets immediately to inform connected network equipment of the IP address and MAC address of the primary unit. The default is 8 seconds, the range is 1 to 20 seconds.

Normally you would not need to change the time interval. However, you could decrease the time to be able to send more packets in less time if your cluster takes a long time to failover.

There may also be a number of reasons to set the interval higher. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully you could increase the interval to reduce the amount of traffic produced after a failover.

## session-pickup {disable | enable}

Enable or disable session pickup. Disabled by default.

Enable session-pickup so that if the primary unit fails, all sessions are picked up by the new primary unit. If you enable session pickup the subordinate units maintain session tables that match the primary unit session table. If the primary unit fails, the new primary unit can maintain most active communication sessions.

If you do not enable session pickup the subordinate units do not maintain session tables. If the primary unit fails all sessions are interrupted and must be restarted when the new primary unit is operating.

Many protocols can successfully restart sessions with little, if any, loss of data. For example, after a failover, users browsing the web can just refresh their browsers to resume browsing. Since most HTTP sessions are very

short, in most cases they will not even notice an interruption unless they are downloading large files. Users downloading a large file may have to restart their download after a failover.

Other protocols may experience data loss and some protocols may require sessions to be manually restarted. For example, a user downloading files with FTP may have to either restart downloads or restart their FTP client.

### **session-pickup-connectionless {disable | enable}**

Enable or disable session synchronization for connectionless (UDP and ICMP) sessions when `mode` is set to `a-a` or `a-p`. When `mode` is standalone, session pickup applies to FGSP cluster TCP session synchronization only. This is available if session-pickup is enabled but by default it is disabled.

### **session-pickup-expectation {disable | enable}**

Enable or disable session synchronization for expectation sessions in an FGSP cluster. This is available if session-pickup is enabled and mode is standalone and is disabled by default.

FortiOS session helpers keep track of the communication of Layer-7 protocols such as FTP and SIP that have control sessions and expectation sessions. Usually the control sessions establish the link between server and client and negotiate the ports and protocols that will be used for data communications. The session helpers then create expectation sessions through the FortiGate for the ports and protocols negotiated by the control session.

The expectation sessions are usually the sessions that actually communicate data. For FTP, the expectation sessions transmit files being uploaded or downloaded. For SIP, the expectation sessions transmit voice and video data. Expectation sessions usually have a timeout value of 30 seconds. If the communication from the server is not initiated within 30 seconds the expectation session times out and traffic will be denied.

### **session-pickup-nat {disable | enable}**

Enable or disable session synchronization for NAT sessions in an FGSP cluster. This is available if session-pickup is enabled and mode is standalone and is disabled by default.

### **session-pickup-delay {disable | enable}**

Enable or disable synchronizing sessions only if they remain active for more than 30 seconds. This option improves performance when session-pickup is enabled by reducing the number of sessions that are synchronized.

### **session-sync-daemon-number <number>**

The number of processes used by the HA session sync daemon. Increase the number of processes to handle session packets sent from the kernel efficiently when the session rate is high. Intended for ELBC clusters, this feature only works for clusters with two members. The default is 1, the range 1 to 15.

### **link-failed-signal {disable | enable}**

Enable or disable shutting down all interfaces (except for heartbeat device interfaces) of a cluster unit with a failed monitored interface for one second after a failover occurs. Enable this option if the switch the cluster is connected to does not update its MAC forwarding tables after a failover caused by a link failure. Disabled by default.

If you choose to disable sending gratuitous ARP packets (by setting `gratuitous-arps` to `disable`) you must first enable `link-failed-signal`. The cluster must have some way of informing attached network devices that a failover has occurred.

### **uninterruptible-upgrade {disable | enable}**

Enable or disable upgrading the cluster without interrupting cluster traffic processing. Enabled by default.

If `uninterruptible-upgrade` is enabled, traffic processing is not interrupted during a normal firmware upgrade. This process can take some time and may reduce the capacity of the cluster for a short time. If is enabled, traffic processing is not interrupted during a normal firmware upgrade. This process can take some time and may reduce the capacity of the cluster for a short time.

If `uninterruptible-upgrade` is disabled, traffic processing is interrupted during a normal firmware upgrade (similar to upgrading the firmware operating on a standalone FortiGate unit).

### **ha-mgmt-status {enable | disable}**

Enable or disable the HA reserved management interface feature. Disabled by default.

### **ha-mgmt-interface <interface\_name>**

The FortiGate interface to be the reserved HA management interface. You can configure the IP address and other settings for this interface using the `config system interface` command. When you enable the reserved management interface feature the configuration of the reserved management interface is not synchronized by the FGCP.

### **ha-mgmt-interface-gateway <gateway\_IP>**

The default route for the reserved HA management interface (IPv4). This setting is not synchronized by the FGCP.

### **ha-mgmt-interface-gateway6 <gateway\_IP>**

The default route for the reserved HA management interface (IPv6). This setting is not synchronized by the FGCP.

### **ha-eth-type <type>**

The Ethertype used by HA heartbeat packets for NAT/Route mode clusters. `<type>` is a 4-digit number. Default is 8890.

### **hc-eth-type <type>**

The Ethertype used by HA heartbeat packets for Transparent mode clusters. `<type>` is a 4-digit number. Default is 8891.

## l2ep-eth-type <type>

The Ethertype used by HA telnet sessions between cluster units over the HA link. <type> is a 4-digit number. Default is 8893.

## ha-uptime-diff-margin <margin>

The cluster age difference margin (grace period). This margin is the age difference ignored by the cluster when selecting a primary unit based on age. Normally the default value of 300 seconds (5 minutes) should not be changed. However, for demo purposes you can use this option to lower the difference margin. The range is 1 to 65535 seconds.

You may want to reduce the margin if during failover testing you don't want to wait the default age difference margin of 5 minutes. You may also want to reduce the margin to allow uninterruptible upgrades to work.

You may want to increase the age margin if cluster unit startup time differences are larger than 5 minutes.

During a cluster firmware upgrade with `uninterruptible-upgrade` enabled (the default configuration) the cluster should not select a new primary unit after the firmware of all cluster units has been updated. But since the age difference of the cluster units is most likely less than 300 seconds, age is not used to affect primary unit selection and the cluster may select a new primary unit.

During failover testing where cluster units are failed over repeatedly the age difference between the cluster units will most likely be less than 5 minutes. During normal operation, if a failover occurs, when the failed unit rejoins the cluster its age will be very different from the age of the still operating cluster units so the cluster will not select a new primary unit. However, if a unit fails and is restored in a very short time the age difference may be less than 5 minutes. As a result the cluster may select a new primary unit during some failover testing scenarios.

## vcluster2 {disable | enable}

Enable or disable virtual cluster 2 (also called secondary-vcluster).

When multiple VDOMs are enabled, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use `config secondary-vcluster` to configure virtual cluster 2.

Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.

Enabling virtual cluster 2 enables `override` for virtual cluster 1 and virtual cluster 2.

## vcluster-id

Indicates the virtual cluster you are configuring. You can't change this setting. You can use the `config secondary-vcluster` command to edit vcluster 2.

## standalone-config-sync {disable | enable}

Synchronize the configuration of the FortiGate unit in an FGSP cluster. This is available if `session-pickup` is enabled and `mode` is `standalone`. Disabled by default.

## override {disable | enable}

Enable or disable forcing the cluster to renegotiate and select a new primary unit every time a cluster unit leaves or joins a cluster, changes status within a cluster, or every time the HA configuration of a cluster unit changes.

Disabled by default. Automatically enabled when you enable virtual cluster 2. This setting is not synchronized to other cluster units.

In most cases you should keep override disabled to reduce how often the cluster negotiates. Frequent negotiations may cause frequent traffic interruptions. However, if you want to make sure that the same cluster unit always operates as the primary unit and if you are less concerned about frequent cluster negotiation you can set its device priority higher than other cluster units and enable `override`.

## priority <priority>

The device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the cluster unit with the highest device priority becomes the primary unit. The device priority range is 0 to 255. The default is 128. This setting is not synchronized to other cluster units. The device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the cluster unit with the highest device priority becomes the primary unit. The device priority range is 0 to 255. The default is 128. This setting is not synchronized to other cluster units.

## override-wait-time <seconds>

Delay renegotiating when override is enabled and HA is enabled or the cluster mode is changed or after a cluster unit reboots. You can add a time to prevent negotiation during transitions and configuration changes. Range 0 to 3600 seconds.

## schedule {hub | ip | ipport | leastconnection | none | random | round-robin | weight-round-robin}

The cluster's active-active load balancing schedule.

- `hub` load balancing if the cluster interfaces are connected to hubs. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet.
- `ip` load balancing according to IP address.
- `ipport` load balancing according to IP address and port.
- `leastconnection` least connection load balancing.
- `none` no load balancing. Use when the cluster interfaces are connected to load balancing switches.
- `random` random load balancing.
- `round-robin` round robin load balancing. If the cluster units are connected using switches, use round-robin to distribute traffic to the next available cluster unit.
- `weight-round-robin` weighted round robin load balancing. Similar to `round robin`, but you can assign weighted values to each of the units in the cluster.

## slave-switch-standby {disable | enable}

Enable to force a subordinate FortiSwitch-5203B or FortiController-5902D into standby mode even though its weight is non-zero. This is a content clustering option and is disabled by default.



## minimum-worker-threshold <threshold>

Available on FortiSwitch-5203Bs or FortiController-5902Ds only in inter-chassis content-cluster mode. In inter-chassis mode the system considers the number of operating workers in a chassis when electing the primary chassis. A chassis that has less than the `minimum-worker-threshold` of workers operating is ranked lower than a chassis that meets or exceeds the `minimum-worker-threshold`. The default value of 1 effectively disables the threshold. The range is 1 to 11.

## monitor <interface-name> [<interface-name>...]

Enable or disable port monitoring for link failure. Port monitoring (also called interface monitoring) monitors FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks.

Enter the names of the interfaces to monitor. Use a space to separate each interface name. Use append to add an interface to the list. If there are no monitored interfaces then port monitoring is disabled.

You can monitor physical interfaces, redundant interfaces, and 802.3ad aggregated interfaces but not VLAN interfaces, IPsec VPN interfaces, or switch interfaces.

You can monitor up to 64 interfaces. In a multiple VDOM configuration you can monitor up to 64 interfaces per virtual cluster.

## pingserver-monitor-interface <interface-name> [<interface-name>...]

Enable HA remote IP monitoring by specifying the FortiGate unit interfaces that will be used to monitor remote IP addresses. You can configure remote IP monitoring for all types of interfaces including physical interfaces, VLAN interfaces, redundant interfaces and aggregate interfaces.

Use a space to separate each interface name. Use append to add an interface to the list.

## pingserver-failover-threshold <threshold>

The HA remote IP monitoring failover threshold. The failover threshold range is 0 to 50. Setting the failover threshold to 0 (the default) means that if any ping server added to the HA remote IP monitoring configuration fails an HA failover will occur.

Set the priority for each remote IP monitoring ping server using the `ha-priority` option of the `config system link-monitor` command. Increase the priority to require more remote links to fail before a failover occurs.

## pingserver-slave-force-reset {disable | enable}

In a remote IP monitoring configuration, if you also want the same cluster unit to always be the primary unit you can set its device priority higher and enable override. With this configuration, when a remote IP monitoring failover occurs, after the flip timeout expires another failover will occur (because override is enabled) and the unit with override enabled becomes the primary unit again. So the cluster automatically returns to normal operation.

The primary unit starts remote IP monitoring again. If the remote link is restored the cluster continues to operate normally. If, however, the remote link is still down, remote link failover causes the cluster to failover again. This will repeat each time the flip timeout expires until the failed remote link is restored.

You can use the `pingserver-slave-force-reset` option to control this behavior. By default this option is enabled and the behavior described above occurs. The overall behavior is that when the remote link is restored the cluster automatically returns to normal operation after the flip timeout.

If you disable `pingserver-slave-force-reset` after the initial remote IP monitoring failover nothing will happen after the flip timeout (as long as the new primary unit doesn't experience some kind of failover). The result is that repeated failovers no longer happen. But it also means that the original primary unit will remain the subordinate unit and will not resume operating as the primary unit.

## pingserver-flip-timeout <timeout>

The HA remote IP monitoring flip timeout in minutes. If HA remote IP monitoring fails on all cluster units because none of the cluster units can connect to the monitored IP addresses, the flip timeout stops a failover from occurring until the timer runs out. The range is 6 to 2147483647 minutes. The default is 60 minutes.

The flip timeout reduces the frequency of failovers if, after a failover, HA remote IP monitoring on the new primary unit also causes a failover. This can happen if the new primary unit cannot connect to one or more of the monitored remote IP addresses. The result could be that until you fix the network problem that blocks connections to the remote IP addresses, the cluster will experience repeated failovers. You can control how often the failovers occur by setting the flip timeout.

The flip timeout stops HA remote IP monitoring from causing a failover until the primary unit has been operating for the duration of the flip timeout. If you set the flip timeout to a relatively high number of minutes you can find and repair the network problem that prevented the cluster from connecting to the remote IP address without the cluster experiencing very many failovers. Even if it takes a while to detect the problem, repeated failovers at relatively long time intervals do not usually disrupt network traffic.

The flip timeout also causes the cluster to renegotiate when it expires unless you have disabled `pingserver-slave-force-reset`.

## vdom <vdom-name> [<vdom-name>...]

Add virtual domains to a virtual cluster. By default all VDOMs are added to virtual cluster 1. Adding a virtual domain to a virtual cluster removes it from the other virtual cluster. You add VDOMs to virtual cluster 1 using the following syntax:

```
config system ha
    set vdom root vdom1
end
```

You add VDOMs to virtual cluster 2 using the following syntax:

```
config system ha
    set secondary-vcluster enable
    config vcluster2
        set vdom root vdom1
    end
end
```

## ha-direct {disable | enable}

Enable to use the HA management interface for management access for sending log messages to FortiAnalyzer, or remote syslog servers, and for SNMP, access to remote authentication servers (for example, RADIUS, LDAP), FortiManager, FortiSandbox and so on.

Disabled by default. Only appears if `ha-mgmt-status` is enabled.

### load-balance-all {disable | enable}

By default, active-active HA load balancing distributes proxy-based security profile processing to all cluster units. Proxy-based security profile processing is CPU and memory-intensive, so FGCP load balancing may result in higher throughput because resource-intensive processing is distributed among all cluster units.

Proxy-based security profile processing that is load balanced includes proxy-based virus scanning, proxy-based web filtering, proxy-based email filtering, and proxy-based data leak prevention (DLP) of HTTP, FTP, IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS, IM, and NNTP, sessions accepted by security policies. Other features enabled in security policies such as Endpoint security, traffic shaping and authentication have no effect on active-active load balancing.

You can enable `load-balance-all` to have the primary unit load balance all TCP sessions. Load balancing TCP sessions increases overhead and may actually reduce performance so it is disabled by default.

### load-balance-udp {disable | enable}

Enable or disable load balancing UDP proxy-based security profile sessions. Load balancing UDP sessions increases overhead so it is also disabled by default.

This content clustering option is available for the FortiSwitch-5203B and FortiController-5902D.

### weight {0 | 1 | 2 | 3} <weight>

The weighted round robin load balancing weight to assign to each unit in an active-active cluster. The weight is set according to the priority of the unit in the cluster. An FGCP cluster can include up to four FortiGates (numbered 0 to 3) so you can set up to 4 weights. The default weights mean that the four possible units in the cluster all have the same weight of 40. The weight range is 0 to 255. Increase the weight to increase the number of connections processed by the FortiGate with that priority.

Weights are assigned to individual FortiGates according to their priority in the cluster. The priorities are assigned when the cluster negotiates and can change every time the cluster re-negotiates.

You enter the weight for each FortiGate separately. For example, if you have a cluster of three FortiGate units you can set the weights for the units as follows:

```
set weight 0 5
set weight 1 10
set weight 2 15
```

### cpu-threshold <weight> <low> <high>

Dynamic weighted load balancing by CPU usage. When enabled fewer sessions will be load balanced to the cluster unit when its CPU usage reaches the high watermark.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

### memory-threshold <weight> <low> <high>

Dynamic weighted load balancing by memory usage. When enabled fewer sessions will be load balanced to the cluster unit when its memory usage reaches the high watermark.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

### http-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of HTTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

### imap-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of IMAP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

### nnntp-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of NNTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

### pop3-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of POP3 proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

## smtp-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of SMTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

## config secondary-vcluster

Configure virtual cluster 2. You must first enable `vcluster2`. Use the following syntax.

```
config secondary-vcluster
  set vcluster-id 2
  set override {disable | enable}
  set priority <priority>
  set override-wait-time <time>
  {set | append} monitor <interface-name> [<interface-name>...]
  {set | append} pingserver-monitor-interface <interface-name> [<interface-name>...]
  set pingserver-failover-threshold <threshold>
  set pingserver-slave-force-reset {disable | enable}
  {set | append} vdom <vdom-name> [<vdom-name>...]
end
```

## system ha-monitor

If the FortiGates in a cluster have VLAN interfaces, you can use this command to monitor all VLAN interfaces and write a log message if one of the VLAN interfaces is found to be down. Once configured, this feature works by verifying that the primary unit can connect to the subordinate unit over each VLAN. This verifies that the switch that the VLAN interfaces are connected to is configured correctly for each VLAN. If the primary unit cannot connect to the subordinate unit over one of the configured VLANs the primary unit writes a link monitor log message indicating that the named VLAN went down (log message id 20099).

```
config system ha-monitor
  edit <name_str>
    set monitor-vlan {enable | disable}
    set vlan-hb-interval <integer>
    set vlan-hb-lost-threshold <integer>
  end
```

### monitor-vlan {enable | disable}

Enable monitor VLANs. Disabled by default

### vlan-hb-interval <integer>

The time between sending VLAN heartbeat packets over the VLAN. The VLAN heartbeat range is 1 to 30 seconds. The default is 5 seconds.

---

**vlan-hb-lost-threshold <integer>**

The number of consecutive VLAN heartbeat packets that are not successfully received across the VLAN before assuming that the VLAN is down. The default value is 3, meaning that if 3 heartbeat packets sent over the VLAN are not received then the VLAN is considered to be down. The range is 1 to 60 packets. A VLAN heartbeat interval of 5 means the time between heartbeat packets is five seconds. A VLAN heartbeat threshold of 3 means it takes  $5 \times 3 = 15$  seconds to detect that a VLAN is down.

---

**system interface**

Configure interface settings.

**vdom <string>**

Vdom name to which this interface belong, default is root.

---

**mode {static | dhcp | pppoe}**

The interface IP addressing: static, from external dhcp or external pppoe.

---

**distance <integer>**

The administrative distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route for the same destination, value between 1 to 255.

---

**priority <integer>**

The priority of routes using this interface, lower priority indicates preferred route for the same destination, value between 0 to 4294967295, available when mode set to DHCP or PPPoE.

---

**dhcp-relay-ip <ip>**

The IP of DHCP relay server.

---

**dhcp-relay-service {disable | enable}**

Disable or enable DHCP relay service on this interface, default is disable.

---

**dhcp-relay-type {regular | ipsec}**

Set a regular or an IPsec relay type on this interface.

---

**dhcp-client-identifier <string>**

Used to override the default DHCP client ID created by the FortiGate.

---

**ip <ip & netmask>**

The interface's IP and subnet mask, syntax: X.X.X.X/24.

---

**allowaccess {ping | https | ssh | snmp | http | telnet | ...}**

Permitted access type on this interface:

- fgfm: FortiManager access.
  - radius-acct: RADIUS accounting access.
  - probe-response: Probe access.
  - capwap: CAPWAP access.
- 

**fail-detect {enable | disable}**

Enable or disable interface failed options.

---

**fail-detect-option {detectserver | link-down}**

Select whether the FortiGate detects interface failure by ping server (detectserver) or port detection (link-down), detectserver is only available in NAT mode.

---

**fail-alert-method {link-failed-signal | link-down}**

Select link-failed-signal or link-down method to alert about a failed link.

---

**fail-alert-interfaces {port1 | port2 | ...}**

The names of the FortiGate interfaces from which the link failure alert is sent for this interface.

---

---

**ipunnumbered <ip>**

The Unnumbered IP used for PPPoE interfaces for which no unique local address is provided. If you have been assigned a block of IP addresses by your ISP you can add any of these IP.

---

**username <string>**

The username of the PPPoE account, provided by your ISP.

---

**password <passwd>**

The PPPoE account's password.

---

**idle-timeout <integer>**

Idle time in seconds after which the PPPoE session is disconnected, 0 for no timeout.

---

**disc-retry-timeout <integer>**

The time in seconds to wait before retrying to start a PPPoE discovery, 0 to disable this feature.

---

**padt-retry-timeout <integer>**

PPPoE Active Discovery Terminate (PADT) timeout in seconds used to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP.

---

**service-name <string>**

Set a name for this PPPoE service.

---

**ac-name <string>**

Set the PPPoE server name.

---

**lcp-echo-interval <integer>**

The time in seconds between PPPoE Link Control Protocol (LCP) echo requests, default is 5.

---



**lcp-max-echo-fails <integer>**

Maximum number of missed LCP echoes before the PPPoE link is disconnected, default is 3.

---

**defaultgw {enable | disable}**

Enable to get the gateway IP from the DHCP or PPPoE server, default is enable.

---

**dns-server-override {enable | disable}**

Disable to prevent this interface from using a DNS server acquired via DHCP or PPPoE, default is enable.

---

**pptp-client {enable | disable}**

Enable or disable the use of point-to-point tunneling protocol (PPTP) client, available in static mode only, default is disable.

---

**pptp-user <string>**

PPTP end user name.

---

**pptp-password <passwd>**

PPTP end user password.

---

**pptp-server-ip <ip>**

PPTP server's IP address.

---

**pptp-auth-type {auto | pap | chap | mschapv1 | mschapv2}**

The server authentication type, default is auto.

---

**pptp-timeout <integer>**

Idle timeout in minutes to shut down the PPTP session, values between 0 to 65534 (65534 minutes is 45 days), 0 for disabled, default is 0.

---

---

**arpforward {enable | disable}**

Enable or disable ARP packets forwarding on this interface, default is enable.

---

**broadcast-forward {enable | disable}**

Enable or disable automatic forwarding of broadcast packets, default is disable.

---

**priority-override {enable | disable}**

Enable or disable fail back to higher priority port once recovered. Once enabled, `priority-override` on redundant interfaces gives greater priority to interfaces that are higher in the member list.

---

**bfd {global | enable | disable}**

Use the global setting, enable, or disable Bidirectional Forwarding Detection (bfd) on this interface, global bfd settings is in config system settings, default is global.

---

**l2forward {enable | disable}**

Enable or disable layer-2 forwarding for this interface, default is disable.

---

**icmp-redirect {enable | disable}**

Enable or disable sending ICMP redirect messages from this interface, FortiGate send ICMP redirect messages to notify the original sender of packets if there is a better route available, default is enable.

---

**vlanforward {enable | disable}**

Enable or disable traffic forwarding between VLANs on this interface, default is disable.

---

**stpforward {enable | disable}**

Enable or disable Spanning Tree Protocol (STP) packets forward. STP creates a spanning tree within a network of connected layer-2 bridges while disabling all other links, leaving a single active path between any two network nodes to prevent any loops which would flood the network.

---

**stpforward-mode {rpl-all-ext-id | rpl-bridge-ext-id | ...}**

Set the STP forward mode:

---

- `rpl-all-ext-id`: Replace all root and bridge extension IDs, the default mode.
  - `rpl-bridge-ext-id`: Replace the bridge extension ID only.
  - `rpl-nothing`: Do not replace any thing.
- 

### `ips-sniffer-mode {enable | disable}`

Enable or disable the use of this interface as a one-armed sniffer as part of configuring a FortiGate unit to operate as an IDS appliance by sniffing packets for attacks without processing packets. When enabled you cannot use the interface for other traffic, default is disable.

---

### `ident-accept {enable | disable}`

Enable or disable passing packets identification on TCP port 113 to the firewall policy used to determine a user's identity on a particular TCP connection, default is disable. Enable or disable passing packets identification on TCP port 113 to the firewall policy used to determine a user's identity on a particular TCP connection, default is disable.

---

### `switch-controller-access-vlan {enable | disable}`

**Note:** This setting's definition has been modified from a previous release.

VLAN access status:

- `enable`: Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.
  - `disable`: Allow normal VLAN traffic.
- 

### `ipmac {enable | disable}`

Enable or disable IP/MAC binding for the specified interface, default is disable. More information available in `config firewall ipmacbinding setting` command.

---

### `subst {enable | disable}`

Enable to always send packets from this interface to the same destination MAC address. Use `substitute-dst-mac` to set the destination MAC address. Disabled by default.

---

### `macaddr <mac>`

Override the factory MAC address of this interface by specifying a new MAC address.

---

---

### substitute-dst-mac <mac>

The destination MAC address that all packets are sent to from this interface if `subst` is enabled.

---

### speed {auto | 10full | 10half | etc }

The interface speed. The default setting and the speeds available depend on the interface hardware. Most often speed is set to `auto` and the interface negotiates with connected equipment to select the best speed. You can set specific speeds if the connected equipment doesn't support negotiation. Some FortiGate interface hardware does not support `auto`. In which case set the interface speed to match the connected network equipment speed.

Enter a space and a "?" after the speed field to display a list of speeds available for your model and interface.

---

### status {up | down}

Start or stop the interface, when stopped, it does not accept or send packets.

If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.

---

### netbios-forward {disable | enable}

Enable to forward Network Basic Input Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server. Enable to forward Network Basic Input Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server.

---

### wins-ip <ip>

The IP address of a WINS server to which NetBIOS broadcasts is forwarded.

---

### type <interface-type>

Enter set type ? to see a list of the interface types that can be created.

---

### mtu-override {enable | disable}

Select `enable` to use custom MTU size instead of default 1500.

---

### mtu <integer>

Set a new MTU value.

---

### wccp {enable | disable}

Enable or disable Web Cache Communication Protocol (WCCP) on this interface, default is disable.

---

### netflow-sampler {disable | tx | rx | both}

Disable or choose how to use netflow on this interface:

- tx: Monitor transmitted traffic.
  - rx: Monitor received traffic.
  - both: Monitor both direction traffic.
- 

### sflow-sampler {enable | disable}

Enable or disable sflow protocol on this interface, default is disable. More information on sflow in `config system sflow` command.

---

### drop-overlapped-fragment {enable | disable}

Enable or disable dropping overlapped packet fragments, default is disable.

---

### drop-fragment {enable | disable}

Enable to drop fragmented packets, default is disable.

---

### scan-botnet-connections {disable | block | monitor}

Disable or choose how to handle connections to botnet servers:

- block: Terminate connections
  - monitor: Log connections.
- 

### sample-rate <integer>

The sample rate defines the average number of packets to wait between samples, value between 10 to 99999. For example, the default sample-rate of 2000 samples 1 of every 2000 packets.

The lower the sample-rate the higher the number of packets sampled. Sampling more packets increases the accuracy of the sampling data but also increases the CPU and network bandwidth required to support sFlow. The default sample-rate of 2000 provides high enough accuracy in most cases.

---

---

### **polling-interval <integer>**

The amount of time in seconds that the sFlow agent waits between sending collected data to the sFlow collector, value between 1 to 255.

A higher polling-interval means less data is sent across the network but also means that the sFlow collector's picture of the network may be out of date, default is 20.

---

### **sample-direction {tx | rx | both}**

Configure the sFlow agent to sample traffic received by the interface (rx) or sent from the interface (tx) or both.

---

### **explicit-web-proxy {enable | disable}**

Enable or disable explicit Web proxy on this interface, default is disable.

---

### **explicit-ftp-proxy {enable | disable}**

Enable or disable explicit FTP proxy on this interface, default is disable.

---

### **tcp-mss <integer>**

The Maximum Size Segment (mss) for TCP connections, it is used when there is an MTU mismatch or DF (Don't Fragment) bit is set.

---

### **inbandwidth <integer>**

The limit of ingress traffic, in Kbit/sec, on this interface, default is 0 which indicate unlimited.

---

### **outbandwidth <integer>**

The limit of egress traffic, in Kbit/sec, on this interface, default is 0 which indicate unlimited.

---

### **spillover-threshold <integer>**

Egress Spillover threshold in kbps used for load balancing traffic between interfaces, range from 0 to 16776000, default is 0.

---

**ingress-spillover-threshold <integer>**

Ingress Spillover threshold in kbps, range from 0 to 16776000, default is 0.

---

**weight <integer>**

Set the default weight for static routes on this interface. This applies when the route has no weight configured.

---

**external {enable | disable}**

Enable or disable identifying if this interface is connected to external side.

---

**config managed-device**

Available when `fortilink` is enabled, used for managed devices through fortilink interface.

**edit <name>**

The identifier of the managed device.

---

**description <string>**

Optionally describe this interface.

---

**alias <string>**

Optionally set an alias which will be displayed with the interface name to make it easier to distinguish.

---

**l2tp-client {enable | disable}**

Enable or disable this interface as a Layer 2 Tunneling Protocol (L2TP) client.

You may need to enable l2forward on this interface, default is disable.

---

**security-mode {none | captive-portal}**

Available when `fortilink` is disabled, `captive-portal` allow access to only authenticated members through this interface.

---

---

**security-mac-auth-bypass {enable | disable}**

Enable or disable MAC address authentication bypass.

---

**security-external-web <string>**

The URL of an external authentication web server, available when `security-mode` is set to `captive-portal`.

---

**security-external-logout <string>**

The URL of an external authentication logout server, available when `security-mode` is set to `captive-portal`.

---

**replacemsg-override-group <group-name>**

Specify replacement message override group name, this is for captive portal messages when `security-mode` is set to `captive-portal`.

---

**security-redirect-url <string>**

Specify URL redirection after captive portal authentication or disclaimer.

---

**security-groups <user-group>**

Optionally, enter the groups that are allowed access to this interface.

---

**security-exempt-list <name>**

Optionally specify the members will bypass the captive portal authentication.

---

**device-identification {enable | disable}**

Enable or disable passive gathering of identity information about source hosts on this interface.

---

**device-user-identification {enable | disable}**

Enable or disable passive gathering of user identity information about source hosts on this interface.

---



**device-identification-active-scan {enable | disable}**

Enable or disable active gathering of identity information about source hosts on this interface.

---

**device-access-list <name>**

Specify the device access list to use which is configured in `config user device-access-list`.

---

**lldp-transmission {enable | disable | vdom}**

Enable, disable, or apply to vdom-level the Link Layer Discovery Protocol (LLDP) transmission for this interface, default is vdom.

---

**fortiheartbeat {enable | disable}**

Enable or disable FortiHeartBeat (FortiTelemetry on GUI) which used to listen for connections from devices with FortiClient installed, default is disable.

---

**broadcast-forticlient-discovery {enable | disable}**

Enable or disable broadcast FortiClient discovery messages, default is disable.

---

**endpoint-compliance {enable | disable}**

Enable or disable endpoint compliance enforcement, default is disabled.

---

**estimated-upstream-bandwidth <integer>**

Estimated maximum upstream bandwidth in kbps, used to estimate link utilization.

---

**estimated-downstream-bandwidth <integer>**

Estimated maximum downstream bandwidth in kbps, used to estimate link utilization.

---

**vrrp-virtual-mac {enable | disable}**

Enable or disable the Virtual Router Redundancy Protocol (VRRP) virtual MAC addresses for the VRRP routers added to this interface, default is disable. See [RFC3768](#) For more information about VRRP.

---

---

## config vrrp

### **vrgrp <integer>**

VRRP group id.

### **vrip <ip>**

IP of the virtual router.

### **priority <integer>**

Virtual router's priority, value between 1 to 255, default is 100.

### **adv-interval <integer>**

Advertisement interval in seconds, value between 1 to 255

### **start-time <integer>**

Startup time in seconds, value between 1 to 255, default is 3.

### **preempt {enable | disable}**

Enable or disable preempt mode, default is enable.

### **vrdst <ip>**

Monitor the route to this destination.

### **status {enable | disable}**

Enabled by default.

---

## **role {lan | wan | dmz | undefined}**

Optionally choose the interface role: lan: Connected to local network of endpoints. wan: Connected to Internet.  
dmz: Connected to server zone. undefined: Interface has no specific role.

---

## **snmp-index <integer>**

Optionally set a permanent SNMP Index of this interface.

---

## **secondary-IP {enable | disable}**

Enable or disable the use of a secondary address on this interface.

---

## config secondaryip

### ip <ip & netmask>

The interface's secondary IP and subnet mask, syntax: X.X.X.X/24.

### allowaccess {ping | https | ssh | snmp | http | telnet | ...}

Permitted access type on this secondary IP:

- fgfm: FortiManager access.
  - radius-acct: RADIUS accounting access.
  - probe-response: Probe access.
  - capwap: CAPWAP access.
- 

### auto-auth-extension-device {enable | disable}

Enable or disable automatic authorization of dedicated Fortinet extension devices on this interface, default is disabled.

### ap-discover {enable | disable}

Enable or disable automatic registration of unknown FortiAP devices, default is disable.

---

### fortilink {enable | disable}

Enable or disable FortiLink on this interface to manage other Fortinet devices such as FortiSwitch.

---

### fortilink-stacking {enable | disable}

Enable or disable FortiLink switch-stacking on this interface.

---

## config ipv6

### ip6-mode {static | dhcp | delegated}

The addressing mode:

- static: Static setting, default mode.
- dhcp: DHCPv6 client.
- delegated: IPv6 address with delegated prefix.

**ip6-dns-server-override {enable | disable}**

Enable or disable using DNS acquired by DHCP.

**ip6-address <ipv6>**

Primary IPv6 address prefix of this interface.

**config ip6-extra-addr****edit <prefix>**

IPv6 address prefix.

**ip6-allowaccess {ping | https | ssh | snmp | http | ...}**

Allow management access to the interface:

- fgfm: FortiManager access.
- capwap: CAPWAP access.

**ip6-send-adv {enable | disable}**

Enable or disable the flag indicating whether or not to send periodic router advertisements and to respond to router solicitations. When enabled, this interface's address will be added to all-routers group (FF02::02) and be included in an Multi Listener Discovery (MLD) report. If no interfaces on the FortiGate unit have ip6-send-advip6-send-adv enabled, the FortiGate unit will only listen to the all-hosts group (FF02::01) which is explicitly excluded from MLD reports according to [RFC 2710](#) section 5.

When disabled (by default), and autoconf is enabled, the FortiGate unit acts as a stateless address auto-configuration client (SLAAC).

**ip6-manage-flag {enable | disable}**

Enable or disable the managed address configuration flag in router advertisements, default is enable.

**ip6-other-flag {enable | disable}**

Enable or disable the other stateful configuration flag in router advertisements, default is enable.

**ip6-max-interval <integer>**

The maximum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface, value between 4 to 1800, default is 600.

**ip6-min-interval <integer>**

The minimum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface, value between 3 to 1350, default is 198.

**ip6-link-mtu <integer>**

The link MTU to be added to the router advertisements options field, 0 means that no MTU options are sent.

**ip6-reachable-time <integer>**

The time, in milliseconds, to be added to the reachable time field in the router advertisements, value between 0 to 3600000, default is 0 which mean no reachable time is specified.

**ip6-retrans-time <integer>**

The number, in milliseconds, to be added to the Retrans Timer field in the router advertisements, default is 0 which mean that the Retrans Timer is not specified.

**ip6-default-life <integer>**

The time, in seconds, to be added to the Router Lifetime field of router advertisements sent from the interface, default is 1800.

**config ip6-prefix-list****edit <prefix>**

Enter the IPv6 prefix you want to configure.

**autonomous-flag {enable | disable}**

Set the state of the autonomous flag for this IPv6 prefix, default is disable.

**onlink-flag {enable | disable}**

Set the state of the on-link flag in this IPv6 prefix, default is disable.

**valid-life-time <integer>**

The valid lifetime in seconds for this IPv6 prefix, default is 2592000 (30 days).

**preferred-life-time <integer>**

The preferred lifetime in seconds, default is 604800 (7 days).

**config ip6-delegated-prefix-list****edit <prefix-id>**

An ID (integer) for this ip6 delegated prefix.

**upstream-interface <interface>**

The interface name from where delegated information is provided.

**autonomous-flag {enable | disable}**

Set the state of the autonomous flag for this IPv6 delegated prefix, default is disable.

**onlink-flag {enable | disable}**

Set the state of the on-link flag in this IPv6 delegated prefix, default is disable.

**subnet <ipv6\_net>**

Subnet to routing prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx

**ip6-hop-limit <integer>**

The number to be added to the Cur Hop Limit field in the router advertisements sent out this interface, default is 0 which mean no hop limit is specified.

**nd-mode {basic | SEND-compatible}**

Neighbor discovery mode, default is basic.

**dhcp6-relay-service {disable | enable}**

Enable or disable DHCP relay service for IPv6.

**dhcp6-relay-type {regular}**

Regular DHCP relay.

**dhcp6-relay-ip <ipv6>**

The IPv6 of one or more DHCP relays.

**dhcp6-prefix-delegation {disable | enable}**

Enable or disable DHCPv6 prefix delegation, default is disable.

**dhcp6-prefix-hint <ipv6\_net>**

DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.

**dhcp6-prefix-hint-plt <integer>**

DHCPv6 prefix hint preferred life time in seconds, default is 604800 (7 days).

**dhcp6-prefix-hint-vlt <integer>**

DHCPv6 prefix hint valid life time in seconds, default is 2592000 (30 days).

---

**config l2tp-client-settings****user <string>**

L2TP user name.

**Password <passwd>**

L2TP password.

**peer-host <string>**

The host name.

**peer-mask <netmask>**

The netmask.

**peer-port <integer>**

The port used to connect to L2TP peers, default is 1701.

**auth-type {auto | pap | chap | mschapv1 | mschapv2}**

Type of authentication used with this client:

- auto— automatically choose type of authentication (default).
- pap — use Password Authentication Protocol.
- chap — use Challenge-Handshake Authentication Protocol.
- mschapv1 — use Microsoft version of CHAP version 1.
- mschapv2 — use Microsoft version of CHAP version 2.

**mtu <integer>**

The Maximum Transmission Unit (MTU), value between 40 and 65535, default is 1460.

**distance <integer>**

The administration distance of learned routes, value between 1 to 255, default is 2.

**priority <integer>**

The routes priority learned through L2TP.

**defaultgw {enable | disable}**

Enable or disable the use the default gateway, default is disable.

## system link-monitor

Use this command to add link health monitors that are used to determine the health of an interface. Link health monitors can also be used for FGCP HA remote link monitoring.

**srcintf <interface>**

The name of the interface to add the link health monitor to.

**server <address> [<address>...]**

One or more IP addresses of the servers to be monitored. If the link health monitor cannot connect to all of the servers remote IP monitoring considers the link to be down. You can add multiple IP addresses to a single link

monitor to monitor more than one IP address from a single interface. If you add multiple IP addresses, the health checking will be with all of the addresses at the same time. The link monitor only fails when no responses are received from all of the addresses.

### **protocol {ping | tcp-echo | udp-echo | http | twamp}**

One or more protocols to be used to test the link. The default is `ping`.

### **gateway-ip <address>**

The IP address of the remote gateway that the link monitor must communicate with to contact the server. Only required if there is no other route on for this communication.

### **source-ip <address>**

Optionally add a source address for the monitoring packets. Normally the source address is the address of the source interface. You can add a different source address if required.

### **interval <interval>**

The time between sending link health check packets. Default is 5 seconds. Range is 1 to 3600 seconds.

### **timeout <timeout>**

The time to wait before receiving a response from the server. Default is 1 second. Range is 1 to 255 seconds.

### **failtime <failover-threshold>**

The number of times that a health check can fail before a failure is detected (the failover threshold). Default is 5. Range is 1 to 10.

### **recoverytime <recovery-threshold>**

The number of times that a health check must succeed after a failure is detected to verify that the server is back up. Default is 5. Range is 1 to 10.

### **ha-priority <priority>**

The priority of this link health monitor when the link health monitor is part of an FGCP remote link monitor configuration. Default is 1. Range is 1 to 50.

### **update-cascade-interface {disable | enable}**

Enable to bring down the source interface if the link health monitor fails. Disable to keep the interface up if the link health monitor fails. Default is enable.



### **update-static-route {disable | enable}**

Enable to remove static routes from the routing table that use this interface if the link monitor fails. Default is enable.

### **status {disable | enable}**

Enable or disable this link health monitor. Default is enable.

## **system np6**

Configure a wide range of settings for your FortiGate's NP6 processors including enabling/disabling fastpath and low latency, enabling session accounting and adjusting session timeouts. As well you can set anomaly checking for IPv4 and IPv6 traffic. You can also configure different settings for each NP6 processor. The settings that you configure for an NP6 processor with the config system np6 command apply to traffic processed by all interfaces connected to that NP6 processor. This includes the physical interfaces connected to the NP6 processor as well as all subinterfaces, VLAN interfaces, IPsec interfaces, LAGs and so on associated with the physical interfaces connected to the NP6 processor.

### **name {np6\_0 | np6\_1 |...}**

Change the settings for one of the FortiGate unit's NP6 processors.

### **fastpath {disable | enable}**

Enable fastpath acceleration to offload sessions to the NP6 processor. You can disable fastpath if you don't want the NP6 processor to offload sessions. Default enable.

### **per-session-accounting {all-enable | disable | enable-by-log}**

Per-session accounting is a logging feature that allows the FortiGate to report the correct bytes/pkt numbers per session for sessions offloaded to an NP6 processor. This information appears in traffic log messages as well as in FortiView. When offloaded sessions appear on the FortiView All Sessions console they include an icon identifying them as NP sessions. You can hover over the NP icon to see some information about the offloaded sessions. By default, per-session accounting is set to `enable-by-log`, which results in per-session accounting being turned on when you enable traffic logging in a policy. You can disable per-session accounting or select `all-enable` to enable per-session accounting for all sessions whether or traffic logging is enabled or not. Per-session accounting can affect NP6 offloading performance. So you should only enable per-session accounting if you need the accounting information. Enabling per-session accounting only supports traffic log messages and does not provide traffic flow data for sFlow or NetFlow.

### **garbage-session-collector {disable | enable}**

Enable deleting expired or garbage sessions. Disabled by default.

### **session-collector-interval <interval>**

Set the expired or garbage session collector time interval in seconds. The range is 1 to 100 seconds. The default is 64 seconds.

### **session-timeout-interval <interval>**

Set the timeout for inactive sessions. The range is 0 to 1000 seconds. The default is 40 seconds.

### **session-timeout-random-range <range>**

Set the random timeout for inactive sessions. The range is 0 to 1000 seconds. The default is 8 seconds.

### **session-timeout-fixed {disable | enable}**

Force session timeouts at fixed instead of random intervals. Disabled by default.

---

## **config fp-anomaly-v4**

Configure how the NP6 processor does IPv4 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called `trap-to-host`). Selecting `trap-to-host` turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy but the anomaly protection is done by the CPU instead of the NP6.

### **tcp-syn-fin {allow | drop | trap-to-host}**

Detect TCP SYN flood SYN/FIN flag set anomalies. Default is `allow`.

### **tcp-fin-noack {allow | drop | trap-to-host}**

Detect TCP SYN flood with FIN flag set without ACK setting anomalies. Default is `trap-to-host`.

### **tcp-fin-only {allow | drop | trap-to-host}**

Detect TCP SYN flood with only FIN flag set anomalies. Default is `trap-to-host`.

### **tcp-no-flag {allow | drop | trap-to-host}**

Detect TCP SYN flood with no flag set anomalies. Default is `allow`.

### **tcp-syn-data {allow | drop | trap-to-host}**

Detect TCP SYN flood packets with data anomalies. Default is `allow`.

### **tcp-winnuke {allow | drop | trap-to-host}**

Detect TCP WinNuke anomalies. Default is `trap-to-host`.

**tcp-land {allow | drop | trap-to-host}**

Detect TCP land anomalies. Default is `trap-to-host`.

**udp-land {allow | drop | trap-to-host}**

Detect UDP land anomalies. Default is `trap-to-host`.

**icmp-land {allow | drop | trap-to-host}**

Detect ICMP land anomalies. Default is `trap-to-host`.

**icmp-frag {allow | drop | trap-to-host}**

Detect Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies. Default is `allow`.

**ipv4-land {allow | drop | trap-to-host}**

Detect IPv4 land anomalies. Default is `trap-to-host`.

**ipv4-proto-err {allow | drop | trap-to-host}**

Detect IPv4 invalid layer 4 protocol anomalies. Default is `trap-to-host`.

**ipv4-unknopt {allow | drop | trap-to-host}**

Detect IPv4 unknown option anomalies. Default is `trap-to-host`.

**ipv4-optrr {allow | drop | trap-to-host}**

Detect IPv4 record route option anomalies. Default is `trap-to-host`.

**ipv4-optssrr {allow | drop | trap-to-host}**

Detect IPv4 strict source record route option anomalies. Default is `trap-to-host`.

**ipv4-optlsrr {allow | drop | trap-to-host}**

Detect IPv4 loose source record route option anomalies. Default is `trap-to-host`.

**ipv4-optstream {allow | drop | trap-to-host}**

Detect IPv4 stream option anomalies.. Default is `trap-to-host`.

**ipv4-optsecurity {allow | drop | trap-to-host}**

Detect IPv4 security option anomalies. Default is `trap-to-host`.

**ipv4-opttimestamp {allow | drop | trap-to-host}**

Detect IPv4 timestamp option anomalies. Default is `trap-to-host`.

---

## config fp-anomaly-v6

Configure how the NP6 processor does IPv6 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called “trap-to-host”). Selecting “trap-to-host” turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy.

### ipv6-land {allow | drop | trap-to-host}

Detect IPv6 land anomalies. Default is `trap-to-host`.

### ipv6-proto-err {allow | drop | trap-to-host}

Detect layer 4 invalid protocol anomalies. Default is `trap-to-host`.

### ipv6-unknopt {allow | drop | trap-to-host}

Detect IPv6 unknown option anomalies. Default is `trap-to-host`.

### ipv6-saddr-err {allow | drop | trap-to-host}

Detect source address as multicast anomalies. Default is `trap-to-host`.

### ipv6-daddr-err {allow | drop | trap-to-host}

Detect IPv6 destination address as unspecified or loopback address anomalies. Default is `trap-to-host`.

### ipv6-optralert {allow | drop | trap-to-host}

Detect IPv6 router alert option anomalies. Default is `trap-to-host`.

### ipv6-optjumbo {allow | drop | trap-to-host}

Detect IPv6 jumbo options anomalies. Default is `trap-to-host`.

### ipv6-opttunnel {allow | drop | trap-to-host}

Detect IPv6 tunnel encapsulation limit option anomalies. Default is `trap-to-host`.

### ipv6-opthomeaddr {allow | drop | trap-to-host}

Detect IPv6 home address option anomalies. Default is `trap-to-host`.

### ipv6-optnsap {allow | drop | trap-to-host}

Detect IPv6 network service access point address option anomalies. Default is `trap-to-host`.

### ipv6-optendpid {allow | drop | trap-to-host}

Detect IPv6 end point identification anomalies. Default is `trap-to-host`.

### ipv6-optinvld {allow | drop | trap-to-host}

Detect IPv6 invalid option anomalies. Default is `trap-to-host`.

## system npu

Configure Network Processor (NP) options for FortiGates with NP6 and NP4 network processors.

### enc-offload-antireplay {disable | enable}

Enable offloading encryption of IPsec anti-replay sessions. Disabled by default. This option is used only when replay detection is enabled in Phase 2 configuration. If replay detection is disabled, encryption is always offloaded.

### dec-offload-antireplay {disable | enable}

Enable offloading decryption of IPsec anti-replay sessions. Enabled by default. This option is used only when replay detection is enabled in Phase 2 configuration. If replay detection is disabled, decryption is always offloaded.

### offload-ipsec-host {disable | enable}

Enable offloading encryption of IPsec local host sessions. Disabled by default. For this option to take effect, FortiOS must have previously sent the security association (SA) to the network processor.

### dedicated-management-cpu {disable | enable}

The GUI and CLI of FortiGate units with NP6 and NP4 processors may become unresponsive when the system is under heavy processing load because NP6 or NP4 interrupts overload the CPUs preventing CPU cycles from being used for management tasks. You can improve GUI and CLI performance in this situation by enabling this option to dedicate CPU core 0 to management tasks. All management tasks are then processed by CPU 0 and NP6 or NP4 interrupts are handled by the remaining CPU cores. Disabled by default.

### np6-cps-optimization-mode {disable | enable}

Enable to operate NP6s in a mode optimized for more connections per second (CPS). Disabled by default.

### capwap-offload {disable | enable}

Enable offloading managed FortiAP and FortiLink CAPWAP sessions to NP6 processors. Enabled by default.

### {ipsec-dec-subengine-mask | ipsec-enc-subengine-mask} <engine-mask>

Use these commands to change the number of IPsec engines used for decryption and encryption. These settings are applied to all of the NP6 processors in the FortiGate unit. <engine-mask> is a hexadecimal number in the range 0x01 to 0xff where each bit represents one IPsec engine. The default <engine-mask> is 0xff which means all IPsec engines are used. Add a lower <engine-mask> to use fewer engines for decryption or encryption. NP6 processors use multiple IPsec engines to accelerate IPsec decryption and encryption. In some cases out of order ESP packets can cause problems if multiple IPsec engines are running. To resolve this problem you can configure all of the NP6 processors to use fewer IPsec engines. to use fewer engines for decryption or encryption. NP6 processors use multiple IPsec engines to accelerate IPsec decryption and encryption. In some

cases out of order ESP packets can cause problems if multiple IPsec engines are running. To resolve this problem you can configure all of the NP6 processors to use fewer IPsec engines.

## system password-policy

Configure a password policy to be used for administrator accounts and/or IPsec VPN pre-shared keys.

### status {enable | disable}

Enable or disable enforcing a password policy. Disabled by default.

---

### apply to {admin-password | ipsec-preshared-key}

Select which passwords must follow the policy. The options are the passwords for administrative accounts, IPsec VPN pre-shared keys, or both. The default is `admin-password`.

---

### minimum-length <int>

Set the minimum number of characters required for a password. The default is 8.

---

### min-lower-case-letter <int>

Set the minimum number of lower case letters that must be used in a password. The default is 0.

---

### min-upper-case-letter <int>

Set the minimum number of upper case letters that must be used in a password. The default is 0.

---

### min-non-alphanumeric <int>

Set the minimum number of non-alphanumeric characters that must be used in a password. The default is 0.

---

### min-number <int>

Set the minimum number of numbers that must be used in a password. The default is 0.

---

### change-4-characters {enable | disable}

Enable or disable to require a new password to differ from the old password by at least four characters. Disabled by default.

---

### expire-status {enable | disable}

Enable or disable password expiration. Disabled by default.

---

### expire-day <int>

Set the number of days after which a password expires. The default is 90. This option only appears when `expire-status` is enabled.

---

### reuse-password {enable | disable}

Enable or disable allowing users to re-use a password. Enabled by default.

## system sms-server

Configure a cellphone service provider to send SMS text messages as part of two-factor authentication.

### mail-server <server\_name>

Set the domain name of the email-to-SMS server.

## system wccp

Use this command to configure various settings for Web Cache Communication Protocol (WCCP). Before you can do this however, you must first configure the FortiGate as either a WCCP router or client: **FortiGate as WCCP router:** Intercepts HTTP and HTTPS sessions and forwards them to a web caching engine, caches web pages, and returns cached content to the web browser. **FortiGate as WCCP client:** Accepts and forwards WCCP sessions and uses firewall policies to apply NAT, UTM, and more security features. Note that FortiGates may only operate as clients while in NAT/Route mode (*not* in Transparent mode). To assign either role to the FortiGate, use the following command:

```
config system settings
    set wccp-cache-engine {enable | disable}
end
```

Set this command to `disable` (by default) for the FortiGate to operate as a WCCP **router**. Set this command to `enable` for the FortiGate to operate as a WCCP **client**. When enabled, an interface named `w.root` is added to the FortiGate (shown under `config system interfaces`). All WCCP sessions received by the FortiGate —

operating as a WCCP client — are considered to be received at this interface, where you can enter firewall policies for WCCP traffic. **Note:** All WCCP entries created, whether for router or client, must be numbered within the range of 0-255. The default is set to 1. Use 0 for HTTP. [toc]

## Router mode

The entries below are available when the FortiGate has been configured as a WCCP router.

### router-id <ip-address>

IP address known to all cache engines, and identifies an interface on the FortiGate to the cache engines. If all cache engines connect to the same FortiGate interface, use the default address of 0.0.0.0. However, if the cache engines can connect to different FortiGate interfaces, you must set `router-id` to a specific IP address, which must then be added to the configuration of the cache engines that connect to that interface.

### group-address <multicast-address>

IP multicast address used by the cache routers. The default, 0.0.0.0, means the FortiGate will ignore multicast WCCP traffic. Otherwise, set the address between 244.0.0.0 to 239.255.255.255.

### server-list <router-1> [router-2] [router-3] [router-4]

IP address and netmask for up to four cache servers.

### authentication {enable | disable}

Enable or disable (by default) use of MD5 authentication for the WCCP configuration.

### password <password>

**Note:** This entry is only available when `authentication` is set to `enable`. Password for MD5 authentication (maximum length of eight characters).

### forward-method {GRE | L2 | any}

Defines how the FortiGate forwards traffic to cache servers:

- **GRE:** Encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP server and a destination IP address of the target WCCP client. This allows the WCCP server to be multiple Layer 3 hops away from the WCCP client.
- **L2:** Rewrites the destination MAC address of the intercepted packet to equal the MAC address of the target WCCP



client. L2 forwarding requires that the WCCP server is Layer 2 adjacent to the WCCP client.

- **any**: Cache server determines the method.
- 

### **return-method {GRE | L2 | any}**

Defines how a cache server declines a redirected packet, and returns it to the FortiGate (see `forward-method` above for option descriptions).

---

### **assignment-method {HASH | MASK | any}**

Defines which assignment method the FortiGate prefers:

- **HASH**: A hash key based on any combination of the source and destination IP and port of the packet.
  - **MASK**: A mask value specified with a maximum of 7 bits and, like the hash key, can be configured to cover both the source and destination address space.
  - **any**: Cache server determines the method.
- 

## **Client mode**

The entries below are available when the FortiGate has been configured as a WCCP client.

### **cache-id <ip-address>**

IP address of the cache engine if its IP address is not the same as the IP address of a FortiGate interface. If the addresses are the same, use the default address of 0 . 0 . 0 . 0.

---

### **group-address <multicast-address>**

IP multicast address used by the cache routers. The default, 0 . 0 . 0 . 0, means the FortiGate will ignore multicast WCCP traffic. Otherwise, set the address between 244 . 0 . 0 . 0 to 239 . 255 . 255 . 255.

---

### **router-list <addresses>**

IP addresses of one or more WCCP routers that can communicate with a FortiGate operating as a WCCP cache engine. Separate multiple addresses with spaces.

---

### **authentication {enable | disable}**

Enable or disable (by default) use of MD5 authentication for the WCCP configuration.

---

---

## cache-engine-method {GRE | L2}

Defines how traffic is forwarded to routers or returned to the cache engine (see `forward-method` above for option descriptions). The default is set to `GRE`.

---

## service-type {auto | standard | dynamic}

WCCP service type, or service group, used by the cache server for logical interception and redirection of traffic. The default is set to `auto`.

- **auto:** Transparent redirection of traffic, whereby the target URL is used to request content, and have requests automatically redirected to a web caching engine.
  - **standard:** Intercepts TCP port 80 (HTTP) traffic to the client.
  - **dynamic:** Use for when the router is instructed which protocol or ports to intercept, and how to distribute the traffic.
- 

## assignment-weight <weight>

Assignment weight/ratio for the WCCP cache engine. Set the value between 0-255. The default is set to 0.

---

## assignment-bucket-format {wccp-v2 | cisco-implementation}

Assignment bucket format for the WCCP cache engine. WCCP version 2 (`wccp-v2`) allows for support of up to 256 masks. The default is set to `cisco-implementation`.

## user

Use `config user` to configure:

- external authentication servers
- user accounts and user groups for firewall policy authentication, SSL VPN authentication, administrator authentication and some types of VPN authentication
- device detection
- peers/peer groups for IPsec VPN and PKI user authentication.

## user adgrp

Configure or edit existing Fortinet Single Sign-On (FSSO) groups. The command below creates a group that defines FSSO agent names and their polling ID.

## server-name <name>

FSSO agent name.

**polling-id <id>**

FSSO polling ID. Set value between 0-4294967295. The default is set to 0.

**user device**

Use this command to define and configure host devices.

**append tags <tag-name>**

Append applied object tags.

---

**mac <mac-address>**

Enter the device's MAC address.

---

**user <name>**

Enter the device owner's user name.

---

**master-device [name]**

Optionally enter a master device name.

---

**comment [string]**

Optional comments.

---

**avatar <image-file>**

Enter an image file name to be used as the user's avatar (maximum 4K base64 encoded).

---

**tags <image-file>**

Enter applied object tags.

---

## type <device-type>

Select the device type from the following:

- android-phone
- android-tablet
- blackberry-phone
- blackberry-playbook
- forticam
- fortifone
- fortinet-device
- gaming-console
- ip-phone
- ipad
- iphone
- linux-pc
- mac
- media-streaming
- printer
- router-nat-device
- windows-pc
- windows-phone
- windows-tablet
- other-network-device

## user device-access-list

Use this command to configure device lists for use on interfaces with device identification enabled.

## config device-list

A configuration method to create device name entries and define their action.

### device <device-group>

Enter the firewall device or device group.

### action {accept | deny}

Accept (by default) or deny the device.

## default-action {accept | deny}

Select whether to accept (by default) or deny unknown/unspecified devices.

## user device-category

Use this command to view all available device types/categories, shown below.

- all
- android-phone
- android-tablet
- blackberry-phone
- blackberry-playbook
- collected-emails
- forticam
- fortifone
- fortinet-device
- gaming-console
- ip-phone
- ipad
- iphone
- linux-pc
- mac
- media-streaming
- other-network-device
- printer
- router-nat-device
- windows-pc
- windows-phone
- windows-tablet

## user device-group

Use this command to edit or define FortiGate default or custom device groups.

### append member <device>

Append device names/categories.

---

### member <group-member>

Enter the device group members that belong to this group, each separated by a space (see the full default [list of device categories](#)).

---

## comment [string]

Optional comments.

## user fortitoken

Use this command to register and view FortiTokens.

## status {active | lock}

Activate (by default) or lock the FortiToken.

---

## comments [string]

Optional comments.

---

## license <license>

Enter the FortiToken Mobile license. You can retrieve the token's license by entering `get`, or by using its activation-code in the following command:

```
execute fortitoken-mobile import <activation-code>
```

---

## activation-code <code>

**Note:** This entry is *not* configurable from the CLI. From the GUI, the token must be assigned to a user and the activation code sent from the FortiGate to the user's email.

---

## activation-expire <expire-time>

**Note:** This entry is *not* configurable from the CLI. From the GUI, the token must be assigned to a user and the activation code sent from the FortiGate to the user's email. The email will tell the user by when they must activate their token.

## user fsso

Use this command to configure the FortiGate unit to receive user group information from a Directory Service server equipped with the Fortinet Single Sign-On (FSSO) Agent. You can specify up to five computers on which an FSSO collector agent is installed. The FortiGate unit uses these collector agents in a redundant configuration, whereby if the first agent fails, the FortiGate unit attempts to connect to the next agent in the list, and so on.

**{server | server2 | server3 | server4 | server5} <agent-address>**

Enter the domain name or IP address for up to five collector agents (maximum of 63 characters).

---

**{port | port2 | port3 | port4 | port5} <agent-port>**

For each collector agent, enter the port number used for communication with FortiGate units. The default, for each port, is set to 8000.

---

**{password | password2 | password3 | password4 | password5} <agent-password>**

For each collector agent, enter the password.

---

**ldap-server <server>**

Enter the name of the LDAP server to be used to get group information from the Directory Service.

---

**source-ip <server>**

Enter the source IP for communications to FSSO servers.

**user fsso-polling**

Use this command to configure polling of servers for FSSO. Edit to define separate ID numbers for the Windows AD server.

**config adgrp**

**Note:** This entry is *not* configurable.

---

**status {enable | disable}**

Enable (by default) or disable FSSO polling.

---

**server <name/ip>**

Name or IP address of the AD server.

---

**default-domain <domain>**

This server's default domain name.

---

**port {port}**

Server port number. Set the value between 0-65535. The default is set to 0.

---

**user <user>**

User name for the AD server.

---

**password <password>**

AD server password.

---

**ldap-server <server>**

Name of the LDAP server for group and user names.

---

**logon-history <hours>**

Amount of time in hours to maintain active logon. Set the value between 1-48 (or one hour to two days). The default is set to 8. Set to 0 to for no time limit.

---

**polling-frequency <frequency>**

Interval time in seconds that polling occurs. Set the value between 1-30. The default is set to 10.

---

**user group**

Use this command to add or edit user groups. User groups can include defined peer users.

**config guest**

**Note:** When `group-type` is set to `guest`, `guest` options will become available and can be set. This configuration method will also become available, however it is *not* configurable.

---



## config match

**Note:** This entry is only available when `group-type` is set to `firewall`. A configuration method to specify the user group names on the authentication servers that are members of this FortiGate user group. Note that if no matches are specified then all users on the server can authenticate.

### server-name <name>

The name of the remote authentication server.

### group-name <name>

The name of the matching group on the remote authentication server.

---

## group-type {firewall | fsso-service | rso | guest}

Type of group, which determines the type of user.

- `firewall`: Those users defined in the `user local`, `user ldap`, or `user radius` commands
  - `fsso-service`: Fortinet Single Sign-On (FSSO) users
  - `rso`: RADIUS Single Sign-On (RSSO) users
  - `guest`: Guest users
- 

## authtimeout <timeout>

Period of time in minutes before the authentication timeout for a user group is reached. Set the value between 1-43200 (or one minute to thirty days). The default is set to 0, which sets the timeout to use the global authentication value.

---

## sso-attribute-value <attribute>

**Note:** This entry is only available when `group-type` is set to `rso`. The name of the RADIUS user group that this local user group represents.

---

## auth-concurrent-override {enable | disable}

**Note:** This entry is only available when `group-type` is set to either `firewall` or `guest`. Enable or disable (by default) overriding the `policy-auth-concurrent` entry in the `system global` command.

---

## auth-concurrent-value <limit>

**Note:** This entry is only available when `auth-concurrent-override` is set to `enable`. The number of concurrent logins permitted from the same user. Set the value between 1-100, or 0 (by default) for unlimited.

---

---

### http-digest-realm <attribute>

**Note:** This entry is *not* available when `group-type` is set to `rssso`. The realm attribute for MD5-digest authentication.

---

### user-id {email | auto-generate | specify}

**Note:** This entry is only available when `group-type` is set to `guest`. The source of the guest user ID.

- `email`: Use the guest's email address (by default).
  - `auto-generate`: Create a random user ID.
  - `specify`: Enter a user ID string.
- 

### password {auto-generate | specify | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. The source of the guest password.

- `auto-generate`: Create a random user password (by default).
  - `specify`: Enter a user password string.
  - `disable`: Disables guest user's need for a password.
- 

### user-name {enable | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. Enable or disable (by default) the guest user name entry.

---

### sponsor {optional | mandatory | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. Determines whether the sponsor field on the web-based manager Guest Management form should be optional (by default), mandatory, or disabled.

---

### company {optional | mandatory | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. Determines whether the guest's company name field on the web-based manager Guest Management form should be optional (by default), mandatory, or disabled.

---

### email {enable | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. Enable (by default) or disable the email address field in the web-based manager Guest Management form.

---

### mobile-phone {enable | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. Enable or disable (by default) the mobile phone number field in the web-based manager Guest Management form.

---

### expire-type {immediately | first-successful-login}

**Note:** This entry is only available when `group-type` is set to `guest`. Determines when the expiry time countdown begins: immediately (by default) or after the user's first successful login.

---

### expire <seconds>

**Note:** This entry is only available when `group-type` is set to `guest`. The time in seconds the user account has until it expires. Set the value between 1-31536000 (or one second to 365 days). The default is set to 14400.

---

### max-accounts <limit>

**Note:** This entry is only available when `group-type` is set to `guest`. The maximum number of accounts permitted. The maximum value that can be set depends on the platform. The default is set to 0, or unlimited.

---

### multiple-guest-add {enable | disable}

**Note:** This entry is only available when `group-type` is set to `guest`. Enable or disable (by default) the multiple guest add option in the web-based manager User Group form.

---

### member <member>

**Note:** This entry is only available when `group-type` is set to either `firewall` or `fsso-service`. The names of users, peers, LDAP servers, or RADIUS servers to add to the user group, each separated by a space. Note that, to add or remove names from the group, you must re-enter the whole list with the required additions or deletions. . The names of users, peers, LDAP servers, or RADIUS servers to add to the user group, each separated by a space. Note that, to add or remove names from the group, you must re-enter the whole list with the required additions or deletions.

## user krb-keytab

Use this command to configure Kerberos keytab entries. Keytab files are used to authenticate to various remote systems using Kerberos without entering a password, and without requiring human interaction or access to password stored in a plain-text file. The script is then able to use the acquired credentials to access files stored on a remote system.

---

**principal <principal>**

The Kerberos service principal, e.g. `HTTP/fgt.example.com@EXAMPLE.COM`.

---

**ldap-server <server>**

The LDAP server name.

---

**keytab <keytab>**

The base64 coded keytab file containing a pre-shared key.

**user ldap**

Use this command to add or edit the definition of an LDAP server for user authentication. The maximum number of remote LDAP servers that can be configured for authentication is 10. LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication. With PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

**append search-type**

Append nested-user-group chain information.

**server <name/ip>**

LDAP server CN domain name or IP address. The host name must comply with [RFC1035](#).

---

**secondary-server [name/ip]**

Optionally, enter a second LDAP server name or IP.

---

**tertiary-server [name/ip]**

Optionally, enter a third LDAP server name or IP.

---

**source-ip [class-ip]**

Optionally, enter a source IP address to be used for LDAP requests.

---

## cnid <id>

Common name identifier for the LDAP server (maximum of 20 characters). The default is set to `cn`, which is the common name identifier for most LDAP servers. However some servers use other common name identifiers such as `uid`.

---

## dn <dn>

**Note:** You must provide a `dn` value if `type` is set to `simple`. Distinguished name used to look up entries on the LDAP server (maximum of 512 characters). The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. The FortiGate unit passes this distinguished name unchanged to the server.

---

## type {simple | anonymous | regular}

**Note:** You must provide a `dn` value if `type` is set to `simple`. Authentication type for LDAP searches.

- `simple`: Simple password authentication without search. Use if the user records are all under one distinguished name that you know. Otherwise, using either `anonymous` or `regular` will search the entire LDAP database for the required user name.
  - `anonymous`: Bind using anonymous user search.
  - `regular`: Bind using username/password and then search. Use if your LDAP server requires authentication to perform searches, providing values for username and password.
- 

## group-member-check {user-attr | group-object | posix-group-object}

Group member checking methods.

- `user-attr`: Check user attributes (by default).
  - `group-object`: Check group objects.
  - `posix-group-object`: Checks Portable Operating System Interface (POSIX) group objects.
- 

## secure {disable | starttls | ldaps}

Port to be used in authentication.

- `disable`: Port 389 (by default)
  - `starttls`: Port 389
  - `ldaps`: Port 636
-

---

### port <port>

Port number to be used for communication with the LDAP server. Set the value between 1-65535. The default is set to 389.

---

### password-expiry-warning {enable | disable}

Enable or disable (by default) password expiry warnings.

---

### password-renewal {enable | disable}

Enable or disable (by default) online password renewal.

---

### member-attr <attribute-name>

Name of attribute from which to get group membership. The default is set to `memberOf`. Examples are shown below: . Examples are shown below:

- `memberOf` for Windows AD and OpenLDAP
  - `groupMembership` for eDirectory
- 

### search-type {nested}

Retrieve the complete nested-user-group chain information of a user in a particular Microsoft AD domain.

---

### account-key-processing {same | strip}

Account key processing operation, an option to keep or strip domain string of User Principal Name (UPN) in the token.

- `same`: Same as UPN. This is set by default.
- `strip`: Strip domain string from UPN.

UPN is a logon method of authentication where you enter the credentials as `username@domainname.com` instead of the Windows authentication method, `domainname\username`.

---

### account-key-name <name>

Account key name, using the UPN as the search filter.

---

## user local

Use this command to add or edit local users and their authentication options, such as two-factor authentication.

**Note:** To add authentication by RADIUS, TACACS+, or LDAP server, you *must* first add servers using the [user radius](#), [user tacacs+](#), or [user ldap](#) commands respectively.

### status {enable | disable}

Enable (by default) or disable allowing the local user to authenticate with the FortiGate unit.

---

### type {password | radius | tacacs+ | ldap}

Method in which the user's password is verified.

- **password:** Once set, enter a password in the `passwd` entry (see entry below). The FortiGate unit will verify the password against this value.
  - **radius:** Once set, enter the server name in the `radius-server` entry (see entry below). The specified RADIUS server will verify the password.
  - **tacacs+:** Once set, enter the server name in the `tacacs+-server` entry (see entry below). The specified TACACS+ server will verify the password.
  - **ldap:** Once set, enter the server name in the `ldap-server` entry (see entry below). The specified LDAP server will verify the password.
- 

### passwd <password>

**Note:** This entry is only available when `type` is set to `password`. The user's password used to authenticate themselves. It is recommended to enter an alphanumeric password of at least six characters in length.

---

### radius-server <server>

**Note:** This entry is only available when `type` is set to `radius`. Enter the name of the RADIUS server with which the user must authenticate.

---

### tacacs+-server <server>

**Note:** This entry is only available when `type` is set to `tacacs+`. Enter the name of the TACACS+ server with which the user must authenticate.

---

---

## ldap-server <server>

**Note:** This entry is only available when `type` is set to `ldap`. Enter the name of the LDAP server with which the user must authenticate. . Enter the name of the LDAP server with which the user must authenticate.

---

## two-factor {disable | fortitoken | email | sms}

Apply two-factor authentication through either FortiToken, email, or SMS, or disable it (by default). If set to `fortitoken`, use the `fortitoken` entry to assign a FortiToken to the user (see entry below).

---

## fortitoken <token>

**Note:** This entry is only available when `two-factor` is set to `fortitoken`. Two-factor recipient's FortiToken serial number. The FortiToken must have already been added to the FortiGate unit to be set here.

---

## email-to <address>

Two-factor recipient's email address.

---

## sms-server {fortiguard | custom}

Send SMS through FortiGuard or other external server.

- `fortiguard`: Send SMS by FortiGuard (by default).
  - `custom`: Send SMS by custom server. Once set, use the `sms-custom-server` entry below to set the external server (see entry below).
- 

## sms-custom-server <server>

**Note:** This entry is only available when `sms-server` is set to `custom`. Name of the custom server to use for SMS-based two-factor authentication. Note that the server must have already been defined using the `system sms-server` command.

---

## sms-phone <number>

User's phone number to be used for SMS-based two-factor authentication.

---

## passwd-policy [policy]

**Note:** This entry is only available when `type` is set to `password`. Optionally, select a password policy to apply to this user. Use the `user password-policy` command to create password policies.

---



## passwd-time

**Note:** This entry is only available when `type` is set to `password`. Displays the time of the last password update in the following format: `<yyyy-mm-dd hh:mm:ss>`.

---

## authtimeout <timeout>

Period of time in minutes before the authentication timeout for a user is reached. Set the value between 1-1440 (or one minute to one day). The default is set to 0, which sets the timeout to use the global authentication value.

---

## workstation <name>

**Note:** This entry is only available when `type` is set to `ldap`. Name of the remote user workstation. Set this value if you want to permit the user to authenticate *only* from a particular workstation.

---

## auth-concurrent-override {enable | disable}

Enable or disable (by default) overriding the `policy-auth-concurrent` entry in the `system global` command.

---

## auth-concurrent-value <limit>

**Note:** This entry is only available when `auth-concurrent-override` is set to `enable`. The number of concurrent logins permitted from the same user. Set the value between 1-100, or 0 (by default) for unlimited.

## user password-policy

Use this command to create password policies that warn users that their password will expire. When a configurable number of days has been reached, the user will have the opportunity to renew their password before the expiration day is reached. Once the policies have been created, you must then apply them to the user with the `passwd-policy` entry under the `user local` command. Password policies can be applied to any user (not just local users), however password policies cannot be applied to a user group.

## expire-days <days>

Period of time in days before the user's password expires. Set the value between 0-999. Default is set to 180.

---

## warn-days <days>

Period of time in days before the user is provided a password expiration warning message upon login. Set the value between 0-30. Default is set to 15.

## user peer

Use this command to add or edit peer (digital certificate holder) information. Peers that you define can be used in the `vpn ipsec phase1` command if `peertype` is set to `peer`. These peers can also be added to peer groups in the `user peergrp` command. This command refers to certificates imported into the FortiGate unit. You can import CA certificates using the `vpn certificate ca` command and local certificates using the `vpn certificate local` command.

## mandatory-ca-verify {enable | disable}

CA certificates installed on the FortiGate unit will check the peer certificate for validity. Enable (by default) or disable to determine what to do if the CA certificate is *not* installed.

- `enable`: Peer will not be authenticated
- `disable`: Peer certificate is automatically considered valid and authenticated

---

## ca <cert-ca>

Name of the CA certificate, as returned by the `execute vpn certificate ca list` command.

---

## subject [constraints]

Optionally, enter any peer certificate name constraints; the name defined here must match the certificate name for successful authentication.

---

## cn <cert-common-name>

Name of the peer certificate common name.

---

## cn-type {string | email | FQDN | ipv4 | ipv6}

Peer certificate common name type.

- `string`: Normal string. This is set by default.
- `email`: User's email address.
- `FQDN`: Fully qualified domain name.

- `ipv4`: User's IPv4 address.
  - `ipv6`: User's IPv6 address.
- 

### **ldap-server <server>**

Name of an LDAP server defined under the `user ldap` command. Performs client access rights check for the defined peer.

---

### **ldap-username <name>**

Login name for the LDAP server.

---

### **ldap-password <password>**

Login password for the LDAP server.

---

### **ldap-mode {password | principal-name}**

Mode for LDAP authentication.

- `password`: Authenticate through user name and password. This is set by default.
  - `principal-name`: Authenticate through LDAP `userPrincipalName` attribute.
- 

### **ocsp-override-server <server>**

Online Certificate Status Protocol (OCSP) server used to retrieve certificates. This applies if OCSP is enabled in the `vpn certificate setting` command.

---

### **two-factor {enable | disable}**

Enable or disable (by default) two-factor authentication, applying certificate and password based authentication. Once set, specify the password to use in the `passwd` entry (see entry below).

---

### **passwd <password>**

**Note:** This entry is only available when `two-factor` is set to `enable`. This peer's password for two-factor authentication.

---

---

## user peergrp

Use this command to add or edit peer groups. Peers that you define can be used in the `vpn ipsec phase1` command if `peertype` is set to `peer`.

### append member <name>

Append peer group members.

---

### member <name>

Member names of the peer group, each separated by a space. To add or remove names from the group, you must re-enter the whole list with the additions or deletions required.

## user pop3

Use this command to configure users who authenticate on a Post Office Protocol 3 (POP3) server. Your Internet server uses the POP3 protocol to receive and hold emails.

### server <name/ip>

Domain name or IP address of the POP3 email server.

---

### port <port>

POP3 service port number. This is set to 110 by default).

---

### secure {none | starttls | pop3s}

Security measure to apply: `none`, `starttls` (by default), or `pop3s` (POP3 over SSL).

## user radius

Use this command to add or edit information used for RADIUS authentication. The default port for RADIUS traffic is 1812. If your RADIUS server uses a different port you can change the default RADIUS port here. You may set different ports for each of your RADIUS servers, of which you can configure a maximum of ten.

**Note:** All RADIUS Single-Sign On (RSSO) and other SSO related entries are only available when `rssso` is set to `enable`.

### server <name/ip>

**Note:** This entry is only available when `rsso` is set to `disable`. RADIUS server domain name or IP address (host name must comply with [RFC1035](#)).

---

### secret <key>

**Note:** This entry is only available when `rsso` is set to `disable`. RADIUS server shared secret key. The key should be a maximum of 16 characters in length.

---

### timeout <timeout>

Period of time in seconds between re-sending authentication requests. Set the value between 1-300. The default is set to 5. These requests occur during the `remoteauthtimeout` period set in the `system global` command.

---

### all-usergroup {enable | disable}

**Note:** This entry is only available when `rsso` is set to `disable`. Enable or disable (by default) automatically including this RADIUS server to all user groups.

---

### use-management-vdom {enable | disable}

**Note:** This entry is only available when `rsso` is set to `disable`. Enable or disable (by default) using the management VDOM to send requests.

---

### nas-ip <ip>

**Note:** This entry is only available when `rsso` is set to `disable`. IP address of FortiGate interface used to communicate with the RADIUS server, and used as `NAS-IP-Address` and `Called-Station-Id` attribute in RADIUS access requests (see the `rsso-endpoint-attribute` entry below for full list of attributes).

---

### acct-interim-interval <seconds>

**Note:** This entry is only available when `rsso` is set to `disable`. Period of time in seconds between each accounting interim update message. Set the value between 600-86400 (or ten minutes to one day). The default is set to 0.

---

---

### radius-coa {enable | disable}

Enable or disable (by default) RADIUS Change of Authorization (CoA), a mechanism that can change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

---

### radius-port <port>

**Note:** This entry is only available when `rsso` is set to `disable`. RADIUS service port number. Set the value between 0-65535. The default is set to 0.

---

### h3c-compatibility {enable | disable}

Enable or disable (by default) compatibility with the H3C's intelligent Management Center (iMC). When enabled, the supplicant requests 802.1X authentication and then sends a second phase security check request to the H3C IMC server.

---

### auth-type {auto | ms\_chap\_v2 | ms\_chap | chap | pap}

**Note:** This entry is only available when `rsso` is set to `disable`. Authentication method for this RADIUS server.

- `auto`: Automatic authentication setting, uses `pap`, `ms_chap_v2`, and `chap`. This is set by default.
  - `ms_chap_v2`: MS-CHAPv2
  - `ms_chap`: MS-CHAP
  - `chap`: Challenge-Handshake Authentication Protocol
  - `pap`: Password Authentication Protocol
- 

### source-ip <ip>

**Note:** This entry is only available when `rsso` is set to `disable`. Source IP for communications to the RADIUS server.

---

### username-case-sensitive {enable | disable}

Enable or disable (by default) implementation of username case-sensitivity.

---

### class <name>

Class attribute name(s).

---

## password-renewal {enable | disable}

Enable or disable (by default) implementation of password renewal.

## rsso {enable | disable}

Enable (or disable by default) RADIUS SSO (RSSO) to set a variety of options and configure an RSSO agent. FortiOS will then accept connections on the port defined in the `rsso-radius-server-port` entry (see entry below).

## rsso-radius-server-port <port>

The connection that FortiOS listens for RADIUS Start and Stop records on this port. Set the value between 0-65535. The default is set to 1813. If necessary, change the UDP port number used by the RADIUS accounting server for sending RADIUS records.

## rsso-radius-response {enable | disable}

Enable (or disable by default) FortiOS to send RADIUS responses after receiving RADIUS Start and Stop records.

## rsso-validate-request-secret {enable | disable}

Enable (or disable by default) FortiOS to verify that the RADIUS secret matches the RADIUS secret in the RADIUS Start or End record. Verifying the RADIUS secret confirms the RADIUS record as valid.

## rsso-secret <password>

RADIUS secret used by the RADIUS accounting server.

## rsso-endpoint-attribute <attribute>

**Note:** All attributes listed below are also available under the `rsso-endpoint-block-attribute` and `sso-attribute` entries. To extract the user end point identifier from the RADIUS Start record, this entry must be set to the name of the RADIUS attribute that contains the end point identifier. The RADIUS attribute must match one of the attributes available. Attributes are case sensitive. The default is set to `Calling-Station-Id`. Select from the table shown below:

User-Name	Login-IP-Host	Called-Station-Id	Acct-Output-Octets
User-Password	Login-Service	Calling-Station-Id	Acct-Session-Id

---

CHAP-Password	Login-TCP-Port	NAS-Identifier	Acct-Authentic
NAS-IP-Address	Reply-Message	Proxy-State	Acct-Session-Time
NAS-Port	Callback-Number	Login-LAT-Service	Acct-Input-Packets
Service-Type	Callback-Id	Login-LAT-Node	Acct-Output-Packets
Framed-Protocol	Framed-Route	Login-LAT-Group	Acct-Terminate-Cause
Framed-IP-Address	Framed-IPX-Network	Framed-AppleTalk-Link	Acct-Multi-Session-Id
Framed-IP-Netmask	State	Framed-AppleTalk-Network	Acct-Link-Count
Framed-Routing	Class	Framed-AppleTalk-Zone	CHAP-Challenge
Filter-Id	Session-Timeout	Acct-Status-Type	NAS-Port-Type
Framed-MTU	Idle-Timeout	Acct-Delay-Time	Port-Limit
Framed-Compression	Termination-Action	Acct-Input-Octets	Login-LAT-Port

---

### rsso-endpoint-block-attribute <attribute>

RADIUS attribute used to block a user. See the `rsso-endpoint-attribute` entry for a full list of the attributes available.

---

### sso-attribute <attribute>

Name of the RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record. The default is set to `Class`. See the `rsso-endpoint-attribute` entry for a full list of the attributes available.

---

### sso-attribute-key <key>

Key prefix for SSO group value in the SSO attribute, with a maximum length of 36 characters.

---

### sso-attribute-value-override {enable | disable}

Enable (by default) or disable overriding old attribute with a new attribute for the same endpoint.

---



### **rsso-context-timeout <seconds>**

Period of time in seconds before the logged on user is removed from the "user context list" of logged on users. Set the value between 1-4294967295 (or one second to 136+ years), or 0 for users you want to remain on the list. The default is set to 28800 (or eight hours). This timeout is only necessary if FortiOS doesn't receive RADIUS Stop records. However it's advisable to set a timeout in case the FortiGate unit misses a Stop record.

---

### **rsso-log-period <seconds>**

Time interval in seconds that FortiOS will generate group event log messages for dynamic profile events. This is to avoid generating groups of event log messages continuously. Each log message contains the number of events of that type occurred. Set the value between 1-4294967295 (or one second to 136+ years), or 0 (by default) to generate all event log messages in real time.

---

### **rsso-log-flags {protocol-error | profile-missing | accounting-stop-missed | accounting-event | endpoint-block | radiusd-other | none}**

Defines how event log messages are written. Multiple options can be set, each separated by a space.

- **protocol-error**: Writes an event log message if RADIUS protocol errors occur. For example, if a RADIUS record contains a RADIUS secret that does not match the one added to the dynamic profile.
  - **profile-missing**: Writes an event log message whenever FortiOS cannot find a group name in a RADIUS Start message that matches the name of an RSSO user group in FortiOS.
  - **accounting-stop-missed**: Writes an event log message whenever a user context entry timeout expires indicating that FortiOS removed an entry from the user context list without receiving a RADIUS Stop message.
  - **accounting-event**: Writes an event log message when FortiOS does not find the expected information in a RADIUS Record. For example, if a RADIUS record contains more than the expected number of addresses.
  - **endpoint-block**: Writes an event log message whenever a user is blocked.
  - **radiusd-other**: Writes an event log message for other events. For example, write a log message if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.
  - **none**: Disable logging of RADIUS SSO events.
- 

### **rsso-flush-ip-session {enable | disable}**

Enable (or disable by default) to flush user IP sessions on RADIUS accounting Stop messages.

---

### **rsso-ep-one-ip-only {enable | disable}**

Enable or disable (by default) the replacement of old IP addresses with new IP addresses for the same endpoint on RADIUS accounting Start messages.

## user security-exempt-list

Use this command to define security exempt rules/lists.

**Note:** To view eligible options for the config options in the entries listed below, enter `set <entry> ?`.

### config rule

A configuration method to create exempt rules. Edit to create new and specify the rule parameters with the entries below.

#### **srcaddr <src-address>**

Source addresses or address groups to be exempted from Captive Portal, each separated by a space.

#### **devices <device>**

Devices or device groups to be exempted from Captive Portal, each separated by a space. These groups can be created/edited using the `user device-group` command.

#### **dstaddr <dst-address>**

Destination addresses or address groups to be exempted from Captive Portal, each separated by a space.

#### **service <dst-service>**

Destination services to be exempted from Captive Portal, each separated by a space.

---

### description [description]

Optional description for the group.

## user setting

Use this command to configure per VDOM user settings such as the firewall user authentication time out and protocol support for firewall policy authentication.

### config auth-ports

A configuration method to set authentication ports and their authentication types. Edit to create new and configure the following entries below.

#### **type {http | https | ftp | telnet}**

User authentication protocol support for firewall policy authentication for the port. User controls which protocols (HTTP, HTTPS, FTP, and/or TELNET) should support the authentication challenge. The default is set to `http`.

---

**port <port>**

Authentication port number. Set the value between 1-65535. The default is set to 1024.

---

**auth-type {http | https | ftp | telnet}**

Select the protocols that can be used for firewall policy authentication. Default is `http https ftp telnet`, which means firewall policy authentication can be done using HTTP, HTTPS, FTP or Telnet. You can remove protocols to limit the authentication options.

---

**auth-cert <cert>**

HTTPS server certificate for policy authentication. Select from built-in defaults or custom certificates. The built-in `Fortinet_Factory` certificate is set by default.

---

**auth-ca-cert <ca-cert>**

If the built-in certificate is not used here, specify the CA certificate to use instead.

---

**auth-secure-http {enable | disable}**

Enable or disable (by default) redirecting HTTP user authentication to more secure HTTPS.

---

**auth-http-basic {enable | disable}**

Enable or disable (by default) support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of an authentication web page. An example to use this would be for web browsers on mobile devices, as some may only support HTTP basic authentication. Enable or disable (by default) support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of an authentication web page. An example to use this would be for web browsers on mobile devices, as some may only support HTTP basic authentication.

---

**auth-multi-group {enable | disable}**

Enable (by default) or disable the retrieval of groups to which a user belongs. You can disable this option if the Active Directory structure is setup such that users belong to only one group.

---

**auth-timeout <minutes>**

Period of time in minutes before the firewall user authentication timeout requires the user to authenticate again. Set the value between 1-1440 (or one minute to one day). To improve security, it's recommended to keep the

authentication timeout at the default value of 5.

---

### **auth-timeout-type {idle-timeout | hard-timeout | new-session}**

Type of authentication timeout.

- `idle-timeout`: Applies only to idle sessions. This is set by default.
  - `hard-timeout`: Uses RADIUS timeout.
  - `new-session`: Applies only to new sessions.
- 

### **auth-portal-timeout <minutes>**

Period of time in minutes before the firewall Captive Portal authentication timeout requires the user to authenticate again. Set the value between 1-30 (or one minute to half an hour). The default is set to 3.

---

### **radius-ses-timeout-act {hard-timeout | ignore-timeout}**

RADIUS session timeout action.

- `hard-timeout`: Uses RADIUS timeout. This is set by default.
  - `ignore-timeout`: Ignores RADIUS timeout.
- 

### **auth-blackout-time <seconds>**

When a firewall authentication attempt fails five times within one minute, the IP address (that is the source of the authentication attempts) is denied access for this period of time in seconds. Set the value between 0-3600 (or no denial to one hour). The default is set to 0. When a firewall authentication attempt fails five times within one minute, the IP address (that is the source of the authentication attempts) is denied access for this period of time in seconds. Set the value between 0-3600 (or no denial to one hour). The default is set to 0.

---

### **auth-invalid-max <failed-attempts>**

Maximum number of failed authentication attempts before the client is blocked. Set the value between 1-100. The default is set to 5.

---

### **auth-lockout-threshold <login-attempts>**

Number of login attempts before a login lockout is triggered. Set the value between 1-10. The default is set to 3.

---

**auth-lockout-duration <seconds>**

Period of time in seconds that login lockout lasts for. Set the value between 1-4294967295 (or one second to 136+ years), or 0 for no lockout.

**user tacacs+**

Use this command to add or edit information used for Terminal Access Controller Access-Control System (TACACS+) authentication, a remote authentication protocol used to communicate with an authentication server. The default port for a TACACS+ server is 49. A maximum of 10 remote TACACS+ servers can be configured, and alternative authentication methods can be set for each server. These methods include CHAP, PAP, MS-CHAP, and ASCII. The host name for TACACS+ servers must comply with [RFC1035](#).

**server <name/ip>**

Name or IP address of the TACACS+ sever.

**secondary-server <name/ip>**

Name or IP address of the second sever.

**tertiary-server <name/ip>**

Name or IP address of the third sever.

**port <port>**

TACACS+ port number for this server. Set the value between 1-65535. The default is set to 49.

**key <key>**

Key used to access the server.

**secondary-key <key>**

Key used to access the second server.

**tertiary-key <key>**

Key used to access the third server.

**authen-type {mschap | chap | pap | ascii | auto}**

Authentication method for this TACACS+ server.

- `mschap`: MS-CHAP
- `chap`: Challenge Handshake Authentication Protocol
- `pap`: Password Authentication Protocol
- `ascii`: American Standard Code for Information Interchange, a protocol that represents characters as numerical values.
- `auto`: Uses PAP, MS-CHAP, and CHAP (in that order). This is set by default.

## authorization {enable | disable}

Enable or disable (by default) TACACS+ authorization.

## source-ip <src-ip>

Enter the source IP address for communications to the TACACS+ server.

## vpn

Use `vpn` commands to configure options related to virtual private networking through the FortiGate unit, including:

- IPsec operating parameters
- a local address range for PPTP or L2TP clients
- SSL VPN configuration settings

## vpn certificate

### certificate ca

Use this command to install Certificate Authority (CA) root certificates. When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the CRL.

#### ca <cert>

Enter or retrieve the CA certificate as a Privacy Enhanced Mail (PEM) file.

---

### range {global | vdom}

Either `global` (by default) or `vdom` IP address range for the CA certificate.

---

### source {factory | user | bundle | fortiguard}

CA certificate source.

- **factory:** Default certificate that came with the FortiGate
- **user:** User certificate (set by default)
- **bundle:** Certificate from a bundle file
- **fortiguard:** Certificate from FortiGuard

---

### trusted {enable | disable}

Enable (by default) or disable as a trusted CA.

---

### scep-url <url>

URL of the Simple Certificate Enrollment Protocol (SCEP) server.

---

### auto-update-days <days>

**Note:** This entry is only available when `scep-url` has been set. Amount of time in days before the FortiGate requests an updated CA certificate. Set to 0 (by default) for no auto-update.

---

### auto-update-days-warning <days>

**Note:** This entry is only available when `scep-url` has been set. Amount of time in days before the FortiGate generates an expiry-warning message. Set to 0 (by default) for no warning.

---

### source-ip <ipv4-address>

IPv4 address used to verify that the request is sent from an expected IP.

---

## vpn certificate crl

Use this command to install a Certificate Revocation List (CRL). When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the CRL.

### crl <pem-file>

The name of the CRL in Privacy Enhanced Mail (PEM) format.

---

### range {global | vdom}

Either `global` (by default) or `vdom` IP address range for the certificate.

---

### source {factory | user | bundle | fortiguard}

CA certificate source.

- **factory:** Default certificate that came with the FortiGate
- **user:** User certificate (set by default)

- **bundle:** Certificate from a bundle file
- **fortiguard:** Certificate from FortiGuard

---

### update-vdom <vdom>

Name of the VDOM for CRL update. This is set to the `root` VDOM by default.

---

### ldap-server <name>

Name of the LDAP server defined in `config user ldap` for CRL auto-update.

---

### ldap-username <name>

**Note:** This entry is only available when `ldap-server` has been set. LDAP login name.

---

### ldap-password <password>

**Note:** This entry is only available when `ldap-server` has been set. LDAP login password.

---

### http-url <url>

URL of an HTTP server used for automatic CRL certificate updates. The URL *must* begin with either **http://** or **https://**.

---

### scep-url <url>

URL of the SCEP server used for automatic CRL certificate updates. The URL *must* begin with either **http://** or **https://**.

---

### scep-cert <cert>

Local certificate used for SCEP communication for CRL auto-update. If a certificate hasn't already been set, the default certificate used is `Fortinet_CA_SSL`.

---

### update-interval <interval>

Period of time in seconds before the FortiGate unit checks for an updated CRL. Enter 0 (by default) to update the CRL only when it expires.

---

### source-ip <ipv4-address>

IPv4 address used to verify that the request is sent from an expected IP.

---

## vpn certificate local

Use this command to install local certificates.

---



**password <password>**

Password in Privacy Enhanced Mail (PEM) format.

---

**comments [string]**

Optional comments.

---

**private-key <key>**

Private key in PEM format, encrypted with the password.

---

**certificate <certificate>**

**Note:** This is only available for local entries that have certificates assigned to them already. Certificate in PEM format.

---

**scep-url <url>**

URL for the Simple Certificate Enrollment Protocol (SCEP) server.

---

**range {global | vdom}**

Either `global` (by default) or `vdom` IP address range for the certificate.

---

**source {factory | user | bundle | fortiguard}**

Select the certificate's source:

- **factory:** Default certificate that came with the FortiGate
  - **user:** User certificate (set by default)
  - **bundle:** Certificate from a bundle file
  - **fortiguard:** Certificate from FortiGuard
- 

**auto-regenerate-days <days>**

**Note:** This entry is only available when `scep-url` has been set. Number of days before expiry that the FortiGate requests an updated local certificate. Set to 0 (by default) for no auto-update.

---

**auto-regenerate-days-warning <days>**

**Note:** This entry is only available when `scep-url` has been set. Number of days before expiry that the FortiGate generates an expiry-warning message. Set to 0 (by default) for no warning.

---

---

**scep-password <password>**

**Note:** This entry is only available when `scep-url` has been set. Password for the SCEP server.

---

**ca-identifier <name>**

**Note:** This entry is only available when `scep-url` has been set. CA identifier of the CA server for signing via SCEP.

---

**name-encoding {printable | utf8}**

**Note:** This entry is only available when `scep-url` has been set. Name encoding method for auto-regeneration:

- **printable:** Printable encoding (also known as Quoted-Printable, or QP encoding) uses printable ASCII alphanumeric characters and the equals (=) sign (set by default).
  - **utf8:** UTF-8 encoding uses all possible characters.
- 

**source-ip <ipv4-addr>**

Source IP address for communications to the SCEP server.

---

**ike-localid <id>**

**Note:** This entry is only available when `ike-localid-type` is set to `fqdn`. Local ID that the FortiGate will use for authentication purposes as a VPN client.

---

**ike-localid-type <type>**

IKE local ID type:

- **asn1dn:** ASN.1 Distinguished Name ID (set by default)
  - **fqdn:** Fully Qualified Domain Name ID
- 

**vpn certificate ocsdp-server**

Use this command to specify the revocation for an Online Certificate Status Protocol (OCSP) server certificate. You can also specify the action to take if the server is not available.

**url <ocsp-url>**

URL of the OCSP server.

---

**cert <name>**

The OCSP server public certificate (one of the remote certificates).

---

**secondary-url <url>**

Secondary URL of the OCSP server.

---

**secondary-cert <name>**

Secondary public certificate of the OCSP server (one of the remote certificates).

---

**unavail-action {revoke | ignore}**

Upon client certification, when the server is *unreachable*, either *revoke* (by default) the certificate or *ignore* OCSP check.

---

**source-ip <ipv4-address>**

Source IP address for communications to the OCSP server.

---

**vpn certificate remote**

Use this command to install remote certificates and configure basic settings. The remote certificates are public certificates without a private key, and used as OCSP server certificates.

**remote <cert>**

Name of the remote certificate, in PEM format.

---

**range {global | vdom}**

Either *global* (by default) or *vdom* IP address range for the certificate.

---

**source {factory | user | bundle | fortiguard}**

Select the certificate's source:

- **factory:** Default certificate that came with the FortiGate
- **user:** User certificate (set by default)
- **bundle:** Certificate from a bundle file
- **fortiguard:** Certificate from FortiGuard

**vpn certificate setting**

Use this command to enable receiving certificates by OCSP.

**ocsp-status {enable | disable}**

Enable or disable (by default) receiving the certificates using the OCSP.

---

---

### ocsp-default-server <server>

The OCSP server to be used by default. This is one of the servers defined in `config vpn certificate ocsp-server`.

---

### check-ca-cert {enable | disable}

Enable (by default) to check the CA certificate and fail the authentication if the certificate is not found.

---

### strict-crl-check {enable | disable}

Enable or disable (by default) strict mode certificate revocation list (CRL) checking. If strict checking is *not* enabled and a certificate is found to be on a CRL list, the certificate can be used, but a warning log message is written. If strict checking is enabled then all authentication actions that use this certificate fail in addition to the warning message being written.

---

### strict-ocsp-check {enable | disable}

Enable or disable (by default) strict mode OCSP checking. If strict checking is *not* enabled and an OCSP server responds with `cert status unknown`, the certificate can be used, but a warning log message is written. If strict checking is enabled then all authentication actions that use this certificate fail in addition to the warning message being written.

---

## vpn ipsec concentrator

In a hub-and-spoke network, policy-based VPN connections to a number of remote peers radiate from a single, central FortiGate unit, or "hub". The hub functions as a concentrator on the network, managing all VPN connections between the peers, or "spokes". VPN traffic passes from one tunnel to the other through the hub. Add IPsec policy-based VPN tunnels to a VPN concentrator, allowing VPN traffic to pass from one tunnel to the other through the FortiGate unit.

**Note:** VPN concentrators are only available in NAT/Route mode.

### src-check {enable | disable}

Enable to check the source address of the phase 2 selector when locating the best matching phase 2 in a concentrator. Disable (by default) to check only the destination selector.

---

### member <name> [name] [name]

Enter the names of up to three VPN tunnels to add to the concentrator, each separated by a space. Members can be tunnels defined in `vpn ipsec phase1` or `vpn ipsec manualkey`.

---

## vpn ipsec forticlient

Configure automatic VPN connection for FortiClient users. FortiClient users who wish to use automatic VPN configuration must be members of a user group. The command below creates a realm that associates the user group with phase 2 VPN configurations.

---

**usergroupname <name>**

Enter the name of a pre-existing user group created for dialup clients.

---

**phase2name <name>**

Enter the name of the pre-existing phase 2 tunnel configuration defined for the dialup-client configuration.

---

**status {enable | disable}**

Enable (by default) or disable IPsec VPN policy distribution.

**vpn ipsec {manualkey-interface | manualkey}**

Use `manualkey-interface` to configure manual keys for a route-based (interface mode) IPsec VPN tunnel. Creating a route-based tunnel automatically creates a virtual IPsec interface on the FortiGate unit. This interface can be modified afterward using the system network interface command, however this command is only available in NAT/Route mode.

You can also use `manualkey` to configure manual keys for IPsec tunnel-mode VPN tunnels that connect a FortiGate unit and a remote client or gateway that is also using manual key. Because the keys are created when you configure the tunnel, no negotiation is required for the VPN tunnel to start. However, the remote client or gateway must use the same encryption and authentication algorithms and keys.

**Note:** To avoid confusion, the various similar authentication and encryption entries vary in availability, depending on which command is used. Among others, the following authentication/encryption entries are *not* available under the `manualkey` command:

- `auth-alg`
- `enc-alg`
- `auth-key`
- `enc-key`
- `local-spi`
- `remote-spi`

**interface <name>**

The name of the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.

---

**ip-version {4 | 6}**

Enter 4 (by default) for IPv4 or 6 for IPv6 encapsulation for gateways.

---

**addr-type {4 | 6}**

Enter 4 (by default) for IPv4 or 6 for IPv6 encapsulation for IP packets.

**remote-gw <ip-addr>**

The IP address of the remote gateway's external interface.

---

## local-gw [sec-ip-addr]

An optional secondary IP address of the interface selected in the `interface` entry used for the local end of the VPN tunnel.

---

## auth-alg <algorithm>

Enter one of the following authentication algorithms:

- `null`
- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

Make sure to use the same algorithm at both ends of the tunnel.

**Note:** The `auth-alg` and `enc-alg` entries cannot both be `null`.

---

## enc-alg <algorithm>

Enter one of the following encryption algorithms:

- `null`
- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.
- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA algorithm may not be available on some FortiGate models. Make sure to use the same algorithm at both ends of the tunnel. **Note:** The `auth-alg` and `enc-alg` entries cannot both be `null`.

---

## auth-key <key>

**Note:** This entry is only available when `auth-alg` is set to either `md5`, `sha1`, or `sha256`. The authentication key in 16-digit (8-byte) segments separated by hyphens. For an MD5 key, enter a 32-digit (16-byte) hexadecimal number: eg: 0102030405060708-090a0b0c0d0e0f10

- For a SHA1 key, enter a 40-digit (20-byte) hexadecimal number. The final segment is only 8-digits (4-bytes).
- For a SHA256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

---

### enc-key <key>

**Note:** This entry is only available when `enc-alg` is set to either `des`, `3des`, `aes128`, `aes192`, or `aes256`. The encryption key in 16-digit (8-byte) segments separated by hyphens.

- For a DES key, enter a 16-digit (8-byte) hexadecimal number.
- For a 3DES key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES128 key, enter a 32-digit (16-byte) hexadecimal number.
- For an AES192 key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

---

### local-spi <hex-number>

The local Security Parameter Index (SPI), a tag that helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the remote SPI at the opposite end of the tunnel.

---

### remote-spi <hex-number>

The remote SPI. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the local SPI at the opposite end of the tunnel.

---

### authentication <algorithm>

Enter one of the following authentication algorithms:

- `null`
- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

Make sure to use the same algorithm at both ends of the tunnel.

**Note:** The `authentication` and `encryption` entries cannot both be `null`.

---

### encryption <algorithm>

Enter one of the following encryption algorithms:

- `null`
- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.

- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.
- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA and seed algorithms may not be available on some FortiGate models. Make sure to use the same algorithm at both ends of the tunnel.

**Note:** The `authentication` and `encryption` entries cannot both be `null`.

---

### **authkey** <key>

**Note:** This entry is only available when `authentication` is set to either `md5`, `sha1`, or `sha256`. The authentication key in 16-digit (8-byte) segments separated by hyphens. For an MD5 key, enter a 32-digit (16-byte) hexadecimal number: eg: 0102030405060708-090a0b0c0d0e0f10

- For a SHA1 key, enter a 40-digit (20-byte) hexadecimal number. The final segment is only 8-digits (4-bytes).
- For a SHA256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

---

### **enckey** <key>

**Note:** This entry is only available when `encryption` is set to either `des`, `3des`, `aes128`, `aes192`, or `aes256`. The encryption key in 16-digit (8-byte) segments separated by hyphens.

- For a DES key, enter a 16-digit (8-byte) hexadecimal number.
- For a 3DES key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES128 key, enter a 32-digit (16-byte) hexadecimal number.
- For an AES192 key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

---

### **localspi** <hex-number>

The local Security Parameter Index (SPI), a tag that helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the remote SPI at the opposite end of the tunnel.

---

### **remotespi** <hex-number>

The remote SPI. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the local SPI at the opposite end of the tunnel.

---

### **npu-offload** {enable | disable}

Enable (by default) or disable offloading of VPN session to a network processing unit (NPU).



## vpn ipsec {phase1-interface | phase1}

Use `phase1-interface` to define a phase 1 definition for a route-based (interface mode) IPsec VPN tunnel that generates authentication and encryption keys automatically. Optionally, you can create a route-based phase 1 definition to act as a backup for another IPsec interface; this is achieved with the `set monitor <phase1>` entry below.

You can also use `phase1` to add or edit IPsec tunnel-mode phase 1 configurations, which define how the FortiGate unit and a remote VPN peer (gateway or client) authenticate themselves to each other as part of establishing the IPsec VPN tunnel.

**Note:** Some entries are *not* available under the `phase1` command, including the following:

- `ip-version`
- `local-gw6`
- `remote-gw6`
- `monitor` (and all other monitor related entries)
- `add-gw-route`
- `auto-discovery-sender` (and all other auto discovery related entries)
- `encapsulation` (and all other encapsulation related entries)
- `childless-ike`

## type {static | dynamic | ddns}

The connection type of the remote gateway:

- Use `static` if the remote VPN peer has a static IP address. Once set, use the `remote-gw` entry to specify the IP address.
- Use `dynamic` if the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE).
- Use `ddns` if the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service. Once set, use the `remotegw-ddns` entry to enter the domain name of the remote VPN peer.

**Note:** `ddns` is *not* available when `ip-version` is set to 6.

---

## interface <out-interface>

Enter the name of the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.

---

## ip-version {4 | 6}

Enter 4 (by default) for IPv4 or 6 for IPv6 encapsulation for gateways.

---

## ike-version {1 | 2}

Enter 1 (by default) for IKEv1 or 2 for IKEv2 protocol version.

---

---

### local-gw [sec-addr-ipv4]

An optional secondary IPv4 IP address of the interface selected in the `interface` entry used for the local end of the VPN tunnel.

---

### local-gw6 [sec-addr-ipv6]

**Note:** This entry is only available when `ip-version` is set to 6. An optional secondary IPv6 IP address of the interface selected in the `interface` entry used for the local end of the VPN tunnel.

---

### remote-gw <addr-ipv4>

**Note:** This entry is only available when `ip-version` is set to 4 and `type` is set to `static`. The IPv4 IP address of the remote gateway's external interface. Note that this entry is not available when `type` is set to `dynamic`.

---

### remote-gw6 <addr-ipv6>

**Note:** This entry is only available when `ip-version` is set to 6. The IPv6 IP address of the remote gateway's external interface.

---

### remotegw-ddns <domain-name>

**Note:** This entry is only available when `ip-version` is set to 4 and `type` is set to `ddns`. The identifier of the remote peer (e.g. an FQDN). This should be used when the remote peer has a static domain name and a dynamic IP address.

---

### keylife <seconds>

The amount of time in seconds before the phase 1 encryption key expires, at which time a new encryption key is generated without service interruption. Set the value between 120-172800 seconds (or two minutes to two days). The default is set to 86400.

---

### certificate <cert-string>

**Note:** This entry is only available when `authmethod` is set to `signature`. Enter the names of up to four signed personal certificates for the FortiGate unit. The certificates must have already been installed on the FortiGate before entering them here.

---

### authmethod {psk | signature}

Enter your preferred authentication method:

- Use `psk` (by default) to authenticate using a pre-shared key. Once set, use the `psksecret` entry to specify the pre-shared key.
  - Use `signature` to authenticate using a certificate. Once set, use the `certificate` entry to specify the name of the certificate.
-

## mode {aggressive | main}

**Note:** This entry is only available when `ike-version` is set to 1. An ID protection mode that establishes a secure channel.

- Use `aggressive` mode when a remote peer or dialup client has a dynamic IP address. If this is not set, the remote peer will be authenticated using an identifier (local ID). Identifying information is exchanged in the clear.
- Use `main` mode (by default) when both peers have static IP addresses. Identifying information is hidden.

## peertype <any | one | peer | peergrp | dialup>

The following `peertype` options are available:

- `any`: Accepts any remote client or peer. Peer IDs are not used for authentication purposes. This is set by default.
- `one`: Authenticates either a remote peer or client that has a dynamic IP address and connects using a unique identifier over a dedicated tunnel, or more than one dialup client that connects through the same tunnel using the same (shared) identifier. Once set, use the `peerid` entry to set the peer ID. If more than one dialup client will be connecting using the same identifier, set `mode` to `aggressive`.
- `peer`: Authenticates one or more certificate holders based on a particular (or shared) certificate. Once set, use the `peer` entry to enter the certificate name. If the remote peer has a dynamic IP address, set `mode` to `aggressive`.
- `peergrp`: Authenticates certificate holders that use unique certificates. In this case, you must create a group of certificate holders for authentication purposes. Once set, use the `peergrp` entry to set the certificate group name. If the remote peer has a dynamic IP address, set `mode` to `aggressive`.
- `dialup`: Authenticates dialup VPN clients that use unique identifiers and/or preshared-keys to connect to the VPN through the same VPN tunnel. In this case, you must create a dialup user group for authentication purposes. Once set, use the `usrgrp` entry to set the user group name. If the dialup clients use unique identifiers and preshared-keys, set `mode` to `aggressive`. If the dialup clients use preshared-keys *only*, set `mode` to `main`.

Availability of these options vary depending on which remote gateway `type` and `authmethod` is used. Below is a table to show which `peertypes` are available under different circumstances:

type		authmethod		peertype
static	>	psk	>	any
		signature	>	any, one, peer, peergrp
dynamic	>	psk	>	any, one, dialup
		signature	>	any, one, peer, peergrp
ddns	>	psk	>	any
		signature	>	any, one, peer, peergrp

## peergrp <peer-group>

**Note:** This entry is only available when `peertype` is set to `peergrp`. Accepts the specified peer group.

---

**peerid <peer-id>**

**Note:** This entry is only available when `peertype` is set to `one`. Accepts the specified peer identity.

---

**peer <cert-name>**

**Note:** This entry is only available when `type` is configured. Accepts the specified peer certificate.

---

**default-gw <addr-ipv4>**

**Note:** This entry is only available when `type` is set to `dynamic` and `ip-version` is set to 4. The IPv4 address of the default route gateway to use for traffic exiting the interface.

---

**default-gw-priority <priority>**

**Note:** This entry is only available when `type` is set to `dynamic`. The priority for the default gateway router. Set the value between 0-4294967295. Default is set to 0.

---

**usrgrp <group-name>**

**Note:** This entry is only available when `peertype` is set to `dialup`. The user group. You must have already configured a user group on the FortiGate unit before entering the group's name here.

---

**monitor [phase1]**

**Note:** This entry is not available when `type` is set to `dynamic`. An optional IPsec interface that can act as a backup for another (primary) IPsec interface. Enter the name of the primary interface. Once set, use the `monitor-hold-down-type` entry to configure recovery timing (further configured with the `monitor-hold-down-delay`, `monitor-hold-down-weekday`, and `monitor-hold-down-time` entries).

The backup interface is only used when the primary interface is unavailable. For this, `dpd` must be enabled (set to either `on-idle` or `on-timeout`).

Note that a primary interface can only have one backup interface and cannot itself act as a backup for another interface.

---

**monitor-hold-down-type {immediate | delay | time}**

**Note:** This entry (and all other sub-entries) is only available once `monitor` is configured. Controls the recovery time method when the primary interface re-establishes.

- Use `immediate` (by default) to have the primary interface be re-established immediately.
  - Use `delay` to configure the number of seconds to wait before recovery once the primary interface is re-established (see the `monitor-hold-down-delay` entry).
  - Use `time` to configure the day of the week and/or the time of day to recover once the primary interface is re-established (see the `monitor-hold-down-weekday` and `monitor-hold-down-time` entries).
-

---

### monitor-hold-down-delay <seconds>

**Note:** This entry is only available when `monitor-hold-down-type` is set to `delay`. Configure the number of seconds to wait before recovery once the primary interface is re-established. Set the value between 0-31536000 (or 0 seconds to 1 year). The default is set to 0.

---

### monitor-hold-down-weekday <day>

**Note:** This entry is only available when `monitor-hold-down-type` is set to `time`. Configure the day of the week to recover once the primary interface is re-established. Set the value to either `everyday`, `sunday` (by default), `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, or `saturday`.

---

### monitor-hold-down-time <time>

**Note:** This entry is only available when `monitor-hold-down-type` is set to `time`. Configure the time of day to recover once the primary interface is re-established. Set the hour and minute values of the day, with a colon to separate the two (between 00:00 and 23:59). The default is set to 00:00 (or midnight).

---

### mode-cfg {enable | disable}

Enable IKE Configuration Method so that compatible clients can configure themselves with settings that the FortiGate unit provides. Disable (by default) to prohibit clients from configuring themselves.

---

### assign-ip {enable | disable}

**Note:** This entry is only available when `mode-cfg` is set to `enable`. Enable (by default) or disable the assignment of an IP address to the IPsec interface.

---

### assign-ip-from {range | dhcp}

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The method by which the IP address will be assigned.

- Use `range` (by default) to assign the IP address from a locally defined range.
  - Use `dhcp` to assign the IP address via DHCP.
- 

### ipv4-start-ip <ipv4-start>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The start of the IPv4 range.

---

### ipv4-end-ip <ipv4-end>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The end of the IPv4 range.

---

---

### ipv4-netmask <ipv4-netmask>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv4 netmask.

---

### dns-mode {manual | auto}

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The DNS server mode.

- Use `manual` (by default) to manually configure the DNS servers.
  - Use `auto` to use default DNS servers.
- 

### ipv4-dns-server1 <server1>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify an IPv4 DNS server, of which you may specify up to three (see entries below).

---

### ipv4-dns-server2 <server2>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a second IPv4 DNS server.

---

### ipv4-dns-server3 <server3>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a third IPv4 DNS server.

---

### ipv4-wins-server1 <server1>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Windows Internet Name Service (WINS) is a central mapping of host names to network addresses. Specify a WINS server, of which you may specify up to two (see entry below).

---

### ipv4-wins-server2 <server2>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a second WINS server.

---

### ipv4-exclude-range

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. A configuration method to exclude IPv4 ranges. Edit to create new and specify the exclude-ranges using the `start-ip` and `end-ip` entries.

---

---

### ipv4-split-include <subnet>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv4 split-include subnets. The addresses must have already been configured on the FortiGate unit before entering their names here.

---

### split-include-service <service>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The split-include services. The services must have already been configured on the FortiGate unit before entering their names here.

---

### ipv6-start-ip <ipv6-start>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The start of the IPv6 range.

---

### ipv6-end-ip <ipv6-end>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The end of the IPv6 range.

---

### ipv6-prefix <ipv6-prefix>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv6 address' prefix. Enter a value between 1-128. The default is set to 128.

---

### ipv6-dns-server1 <server1>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify an IPv6 DNS server, of which you may specify up to three (see entries below).

---

### ipv6-dns-server2 <server2>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a second IPv6 DNS server.

---

### ipv6-dns-server3 <server3>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a third IPv6 DNS server.

---

### ipv6-exclude-range

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. A configuration method to exclude IPv6 ranges. Edit to create new and specify the exclude-ranges using

---

the `start-ip` and `end-ip` entries.

---

### ipv6-split-include <subnet>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv6 split-include subnets. The addresses must have already been configured on the FortiGate unit before entering their names here.

---

### unity-support {enable | disable}

**Note:** This entry is only available when `mode-cfg` is set to `enable`. Enable (by default) or disable support for Cisco Unity configuration method extensions.

---

### domain <domain>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The default DNS domain for Unity clients.

---

### banner <message>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The message that Unity clients should display after connecting.

---

### include-local-lan {enable | disable}

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Enable or disable (by default) allowing local LAN access on Unity clients.

---

### client-auto-negotiate {enable | disable}

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Enable or disable (by default) allowing the VPN client to bring up the tunnel when there is no traffic.

---

### client-keep-alive {enable | disable}

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Enable or disable (by default) allowing the VPN client to keep the tunnel up when there is no traffic.

---

### backup-gateway <address>

**Note:** This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The backup gateway address(es) for Unity clients.

---



### proposal <phase1-proposal>

A minimum of one and maximum of ten encryption-message combinations for the phase 1 proposal, for example `aes128-sha256`. Use a space to separate the combinations. Make sure that the remote peer is configured to use at least one of the proposals defined. **Note:** This entry is *not* available if `suite-b` has been configured. Use any of the following key encryption algorithms: has been configured. Use any of the following key encryption algorithms:

- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.
- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA and seed algorithms may not be available on some FortiGate models. Combine key encryptions with any one of the following message digests, to check the authenticity of messages during an encrypted session:

- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

---

### add-route {disable | enable}

**Note:** This entry is only available when `type` is set to `dynamic`. Enable (by default) or disable adding a route to the destination of the peer selector.

---

### exchange-interface-ip {enable | disable}

Enable or disable (by default) the exchange of IPsec interface IP address.

---

### add-gw-route {enable | disable}

Enable to automatically add a route to the remote gateway specified in the `remote-gw` entry. This is disabled by default.

**Note:** This command is deprecated. Instead, use the `dynamic-gateway {enable | disable}` entry in the `config router static` command.

---

---

### psksecret <preshared-key>

**Note:** This entry is only available when `authmethod` is set to `psk`. Enter the pre-shared key. The pre-shared key must be the same on the remote VPN gateway or client and should only be known by network administrators. The key must consist of at least six characters. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

---

### keepalive <seconds>

**Note:** This entry is only available when `nattraversal` is set to `enable`. Set the NAT traversal keepalive frequency in seconds, a period of time that specifies how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until phase 1 and 2 security associations (SAs) expire. Set the value between 10-900 seconds (or ten seconds to 15 minutes). The default is set to 5.

---

### distance <distance>

**Note:** This entry is only available when `type` is set to `dynamic`, or when `mode-cfg` is set to `enable`. The distance for routes added by IKE. Set the value between 1-255. Default is set to 15.

---

### priority <priority>

**Note:** This entry is only available when `type` is set to `dynamic`, or when `mode-cfg` is set to `enable`. The priority for routes added by IKE. Set the value between 0-4294967295. Default is set to 0.

---

### localid <local-id>

**Note:** If you set a local ID on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup server and specify the identifier as a peer ID on the FortiGate dialup server. The local ID, or unique identifier, that the FortiGate uses as a VPN client for authentication purposes.

---

### localid-type {auto | fqdn | user-fqdn | keyid | address}

Determines the type of local ID to be set:

- `auto`: Selects type automatically.
  - `fqdn`: Uses a Fully Qualified Domain Name (FQDN).
  - `user-fqdn`: Uses a User FQDN.
  - `keyid`: Uses Key Identifier ID.
  - `address`: Uses IP address ID.
- 

### auto-negotiate {enable | disable}

Enable (by default) to keep attempting IKE SA negotiation even if the link is down. This feature is useful in cases where there are multiple redundant tunnels but you prefer the primary connection if it can be established.

---

**negotiate-timeout <seconds>**

The amount of time in seconds that the FortiGate unit will wait for the IKE SA to be negotiated. Set the value between 1-300 seconds (or one second to five minutes). The default is set to 5.

---

**fragmentation {enable | disable}**

**Note:** This entry is only available when `ike-version` is set to 1. Enable (by default) intra-IKE fragmentation support on re-transmission of fragmented packets.

---

**dpd {disable | on-idle | on-demand}**

Disable or set Dead Peer Detection (DPD) to either `on-idle` or `on-demand` (by default). DPD detects the status of the connection between VPN peers, cleans up dead connections, and helps establish new VPN tunnels. Note that DPD cannot be used unless both VPN peers support and enable the feature.

- `on-idle`: DPD is triggered when IPsec is idle/inactive.
  - `on-demand`: DPD is triggered when IPsec traffic is sent but no reply is received from the peer.
- 

**dpd-retrycount <retry-integer>**

**Note:** This entry is only available when `dpd` is set to `enable`. The number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the SA. Set the value between 0-10. The default is set to 3. To avoid false negatives set the retry count to a sufficiently high value for your network.

---

**dpd-retryinterval <seconds> [milliseconds]**

**Note:** This entry is only available when `dpd` is set to `enable`. The amount of time in seconds (and optionally milliseconds) that the local VPN peer waits between sending DPD probes. Use a space to separate the seconds and milliseconds (e.g. for 2.5 seconds, enter `2 500`). Set the value between 0-60 seconds and 0-999 milliseconds.

---

**forticlient-enforcement {enable | disable}**

Enable to only permit FortiClient users to connect. Disable (by default) to lift this restriction.

---

**comments [string]**

Optional comments.

---

**npu-offload {enable | disable}**

Enable (by default) or disable offloading of VPN session to a network processing unit (NPU).

---

---

### send-cert-chain {enable | disable}

**Note:** This entry is only available when `authmethod` is set to `signature`. Enable (by default) or disable sending certificate chain.

---

### dhgrp {1 2 5 14 15 16 17 18 19 20 21}

Apply one or more Diffie-Hellman (DH) group numbers, in order of preference, separated by spaces. DH groups determine the strength of the key used in the key exchange process, with higher group numbers being more secure, but requiring additional time to compute the key. Set the value to any one (or more) of the following: 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, and 21. The default is set to 14 5. Note that at least one of the group numbers set on the remote peer or client must be identical to one of the selections on the FortiGate unit. Note that at least one of the group numbers set on the remote peer or client must be identical to one of the selections on the FortiGate unit.

**Note:** This entry is *not* available if `suite-b` has been configured.

---

### suite-b {disable | suite-b-gcm-128 | suite-b-gcm-256}

Disable (by default) or set Suite B to either `suite-b-gcm-128` or `suite-b-gcm-256`. Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels (see [RFC 6379](#), [Suite B Cryptographic Suites for IPsec](#)).

- Suite-B-GCM-128 applies Advanced Encryption Standard (AES) encryption with 128-bit keys and 16-octet integrity check value (OCV) in Galois/Counter Mode (GCM), a mode of operation for symmetric key cryptographic block ciphers. Key establishment uses DH group 19.
  - Suite-B-GCM-256 applies AES encryption with 256-bit keys and 16-octet ICV in GCM. Key establishment uses DH group 20.
- 

### eap {enable | disable}

**Note:** This entry is only available when `ike-version` is set to 2. Enable or disable (by default) IKEv2 Extensible Authentication Protocol (EAP) authentication.

---

### eap-identity {use-id-payload | send-request}

**Note:** This entry is only available when `eap` is set to `enable`. The IKEv2 EAP peer identity type.

- `use-id-payload` uses IKEv2 identity payload to resolve peer identity. This is set by default.
  - `send-request` uses EAP identity request to resolve peer identity.
- 

### acct-verify {enable | disable}

**Note:** This entry is only available when `eap` is set to `enable`. Enable or disable (by default) the verification of RADIUS accounting record.

---

## wizard-type <wizard-type>

Set to one of the following GUI VPN Wizard template types:

- `custom`: Custom VPN configuration.
- `dialup-forticlient`: Dialup for FortiClient Windows, Mac, and Android.
- `dialup-ios`: Dialup for iPhone and/or iPad Native IPsec Client.
- `dialup-android`: Dialup for Android Native IPsec Client.
- `dialup-windows`: Dialup for Windows Native IPsec Client.
- `dialup-cisco`: Dialup for Cisco IPsec Client.
- `static-fortigate`: Site to Site for FortiGate.
- `dialup-fortigate`: Dialup for FortiGate.
- `static-cisco`: Site to Site for Cisco.
- `dialup-cisco-fw`: Dialup for Cisco Firewall.

---

## xauthtype [disable | client | pap | chap | auto]

**Note:** This entry is only available when `ike-version` is set to 1. Optionally configure XAuth (eXtended Authentication). XAuth provides the mechanism for requesting individual authentication information from the user, while a local user database or an external authentication server (such as a RADIUS server) provides a method for storing the authentication information centrally in the local network. This command is disabled by default. Use `pap`, `chap`, or `auto` to configure the FortiGate unit as an XAuth server. Note that these options are only available when `type` is set to `dynamic`.

- `disable`: Disables XAuth.
- `client`: Enable to configure the FortiGate as an XAuth client. Once set, use the `authusr` and `authpasswd` entries to add the XAuth user name and password (see entries below).
- `pap`: Password Authentication Protocol (PAP). Once set, use the `authusrgrp` field to specify the user group containing members that will be authenticated using XAuth.
- `chap`: Challenge Handshake Authentication Protocol (CHAP). Once set, use the `authusrgrp` field to specify the user group containing members that will be authenticated using XAuth.
- `auto`: Enable as server auto. Once set, use the `authusrgrp` field to specify the user group containing members that will be authenticated using XAuth.

---

## reauth {enable | disable}

**Note:** This entry is only available when `ike-version` is set to 2. Enable or disable (by default) re-authentication upon IKE SA lifetime expiration.

---

## authusrgrp <group-name>

**Note:** This entry is only available when `eap` is set to `enable`. The authentication user group. You must have already configured a user group on the FortiGate unit before entering the group's name here.

---

## authusr <name>

**Note:** This entry is only available when `xauthtype` has been configured. Enter the XAuth user name.

---

### authpasswd <password>

**Note:** This entry is only available when `xauthtype` has been configured. Enter the XAuth user's password (maximum of 35 characters).

---

### mesh-selector-type {disable | subnet | host}

**Note:** This entry is only available when `ike-version` is set to 1. Disable (by default) or set dynamic mesh selectors for IKEv1 VPNs to either `subnet` or `host`. Note that dynamic selectors are *not* saved to the configuration and will be removed when tunnels are flushed.

- Use `subnet` to install selector for the address group that matches traffic packets.
  - Use `host` to install selector for the source and destination IP addresses of traffic packets.
- 

### idle-timeout {enable | disable}

Enable or disable (by default) IPsec tunnel to timeout when idle. Once enabled, use the `idle-timeoutinterval` entry to set the period of time the VPN will wait before timing out (see entry below).

---

### idle-timeoutinterval <minutes>

**Note:** This entry is only available when `idle-timeout` is set to `enable`. Enter the IPsec tunnel idle timeout in minutes. Set the value between 10-43200 (or ten minutes to 30 days). The default is set to 15.

---

### ha-sync-esp-seqno {enable | disable}

Enable (by default) or disable the Extended Sequence Number (ESP) jump ahead for IPsec HA. Enabling this feature helps to synchronize the IPsec SA replay counters between newly active HA cluster members and the peer (see RFC 6311, Protocol Support for High Availability of IKEv2/IPsec).

---

### auto-discovery-sender {enable | disable}

Auto Discovery VPN (ADVPN) allows a shortcut to be created between two VPN peers, establishing dynamic on-demand tunnels between each other to avoid routing through the topology's hub device. Enable or disable (by default) sending auto-discovery short-cut messages.

---

### auto-discovery-receiver {enable | disable}

Enable or disable (by default) accepting auto-discovery short-cut messages (see the `auto-discovery-sender` entry above about Auto Discovery).

---

### auto-discovery-forwarder {enable | disable}

Enable or disable (by default) forwarding auto-discovery short-cut messages (see the `auto-discovery-sender` entry above about Auto Discovery).

---

---

### auto-discovery-psk {enable | disable}

**Note:** This entry is only available when `authmethod` is set to `signature` and `auto-discovery-sender` is set to `enable`. Enable or disable (by default) the use of pre-shared keys for the authentication of auto-discovery tunnels.

---

### encapsulation {none | gre | vxlan}

**Note:** This entry is *not* available when `type` is set to `dynamic`. Disable (by default; `none`) or set encapsulation to either `gre` or `vxlan`. Both GRE and VXLAN segmentation scale well together as they allow overlapping subnets and IP ranges. VXLAN is encapsulated in UDP frames, resulting in efficiently distributed traffic. Once set, use the `.` Both GRE and VXLAN segmentation scale well together as they allow overlapping subnets and IP ranges. VXLAN is encapsulated in UDP frames, resulting in efficiently distributed traffic. Once set, use the `encapsulation-address` entry to configure the source for the GRE or VXLAN tunnel address.

---

### encapsulation-address {ike | ipv4 | ipv6}

**Note:** This entry is only available when `encapsulation` is set to either `gre` or `vxlan`. Select the source for the GRE or VXLAN tunnel address.

- Use `ike` (by default) to use IKE/IPsec gateway addresses.
  - Use `ipv4` to specify separate IPv4 GRE/VXLAN tunnel addresses (see `encap` entries below).
  - Use `ipv6` to specify separate IPv6 GRE/VXLAN tunnel addresses (see `encap` entries below).
- 

### encap-local-gw4 <addr-ipv4>

**Note:** This entry is only available when `encapsulation-address` is set to `ipv4`. The local IPv4 address of the GRE/VXLAN tunnel.

---

### encap-remote-gw4 <addr-ipv4>

**Note:** This entry is only available when `encapsulation-address` is set to `ipv4`. The remote IPv4 address of the GRE/VXLAN tunnel.

---

### encap-local-gw6 <addr-ipv6>

**Note:** This entry is only available when `encapsulation-address` is set to `ipv6`. The local IPv6 address of the GRE/VXLAN tunnel.

---

### encap-remote-gw6 <addr-ipv6>

**Note:** This entry is only available when `encapsulation-address` is set to `ipv6`. The remote IPv6 address of the GRE/VXLAN tunnel.

---

### **nattraversal {enable | disable}**

Enable (by default) or disable NAT traversal. This should be enabled if you expect the IPsec VPN traffic to go through a gateway that performs NAT. If not NAT device is detected, enabling NAT traversal has no effect. Once enabled, use the `keepalive` entry to set the NAT traversal keepalive frequency. Note that both ends of the VPN must have the same NAT traversal settings.

---

### **fragmentation-mtu <frag-integer>**

**Note:** This entry is only available when `ike-version` is set to 2. The IKE fragmentation maximum transmission unit (MTU). Set the value between 500-16000. The default is set to 1200.

---

### **childless-ike {enable | disable}**

**Note:** This entry is only available when `ike-version` is set to 2. Enable or disable the childless IKEv2 initiation (see RFC 6023, A Childless of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)).

## **vpn ipsec {phase2-interface | phase2}**

Use `phase2-interface` to add or edit a phase 2 configuration on a route-based (interface mode) IPsec tunnel. This command is only available in NAT/Route mode. You can also use `phase2` to add or edit IPsec tunnel-mode phase 2 configurations to create and maintain IPsec VPN tunnels with a remote VPN gateway or client peer. **Note:** The following entries are *not* available under the `phase2` command:

- `auto-discovery-sender`
- `auto-discovery-forwarder`

### **phase1name <gateway\_name>**

The name of the phase 1 gateway configuration, most commonly created using the IPsec Wizard. You must have already added the phase 1 gateway definition to the FortiGate configuration before it can be added here.

---

### **dhcp-ipsec {enable | disable}**

Enable or disable (by default) DHCP-IPsec.

---

### **use-natip {enable | disable}**

Enable (by default) or disable the FortiGate to use its public interface IP address as the source selector when outbound NAT is used.

---

### **selector-match {exact | subset | auto}**

The match-type to use when comparing selectors.

- Use `exact` to match selectors exactly.
- Use `subset` to match selectors by subset.
- Use `auto` (by default) to use subset or exact match depending on the selector address type.



### proposal <phase2\_proposal>

A minimum of one and maximum of ten encryption-message combinations for the phase 2 proposal, for example `aes128-sha256`. Use a space to separate the combinations. Make sure that the remote peer is configured to use at least one of the proposals defined. Use any of the following key encryption algorithms:

- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.
- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA and seed algorithms may not be available on some FortiGate models. Combine key encryptions with any one of the following message digests, to check the authenticity of messages during an encrypted session: The ARIA and seed algorithms may not be available on some FortiGate models. Combine key encryptions with any one of the following message digests, to check the authenticity of messages during an encrypted session:

- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

### pfs {enable | disable}

Enable (by default) or disable perfect forward secrecy (PFS). When enabled, encrypted communications and sessions recorded in the past cannot be retrieved and decrypted, should long-term secret keys or passwords be compromised in the future.

### dhgrp {1 2 5 14 15 16 17 18 19 20 21}

Apply one or more Diffie-Hellman (DH) group numbers, in order of preference, separated by spaces. DH groups determine the strength of the key used in the key exchange process, with higher group numbers being more secure, but requiring additional time to compute the key. Set the value to any one (or more) of the following: 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, and 21. The default is set to 14 5.

Note that at least one of the group numbers set on the remote peer or client must be identical to one of the selections on the FortiGate unit.

### replay {enable | disable}

Enable (by default) or disable replay attack detection. When enabled, replay detection discards received packets if they contain a sequence number before the current window, in which case they are seen as being too old, or if

they contain a sequence number which has already been received by the FortiGate unit.

---

### **keepalive {enable | disable}**

Enable or disable (by default) the NAT traversal keepalive frequency, a period of time that specifies how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until phase 1 and 2 security associations (SAs) expire.

---

### **add-route {phase1 | enable | disable}**

Enable, disable, or set to `phase1` (by default) to add route according to phase add-route settings.

---

### **auto-negotiate {enable | disable}**

Enable to keep attempting IKE SA negotiation even if the link is down. This feature is useful in cases where there are multiple redundant tunnels but you prefer the primary connection if it can be established. This is set to `Enable` to keep attempting IKE SA negotiation even if the link is down. This feature is useful in cases where there are multiple redundant tunnels but you prefer the primary connection if it can be established. This is set to `disable` by default.

---

### **auto-discovery-sender {phase1 | enable | disable}**

Auto Discovery VPN (ADVPN) allows a shortcut to be created between two VPN peers, establishing dynamic on-demand tunnels between each other to avoid routing through the topology's hub device. Enable or disable sending auto-discovery short-cut messages, or set to `phase1` (by default) to forward short-cut messages according to the `phase1 auto-discovery-sender` setting.

---

### **auto-discovery-forwarder {phase1 | enable | disable}**

Enable or disable forwarding auto-discovery short-cut messages (see the `auto-discovery-sender` entry above about Auto Discovery), or set to `phase1` (by default) to forward short-cut messages according to the `phase1 auto-discovery-forwarder` setting.

---

### **keylifeseconds <seconds>**

The amount of time in seconds before the phase 2 encryption key expires, at which time a new encryption key is generated without service interruption. Set the value between 120-172800 seconds (or two minutes to two days). The default is set to 86400.

---

### **keylifekbs <bytes>**

The number of bytes before the phase 2 encryption key expires, at which point a new encryption key is generated without service interruption. Set the value between 5120-4294967295 bytes (or 5.12KB to 4.29GB). The default is set to 5120. While it is possible to set the value to lower than the default, it is not recommended.

### keylife-type {seconds | kbs | both}

The phase 2 encryption key expiration type, used to determine when/how a new encryption key is generated without service interruption. Use `seconds` to then set the key life in seconds, or `kbs` to set the key life in kilobytes (see keylife entries above). Use `both` to be able to set both parameters.

---

### single-source {enable | disable}

**Note:** This entry is *not* available when `l2tp` is set to `enable`. Enable or disable (by default) single source IP restrictions.

- `enable` only accepts single source IPs.
  - `disable` accepts source IP range.
- 

### route-overlap {use-old | use-new | allow}

**Note:** This entry is *not* available when `l2tp` is set to `enable`. The action taken for overlapping routes.

- `use-old` uses the old route and does not add the new route.
  - `use-new` deletes the old route and adds the new route.
  - `allow` permits overlapping routes.
- 

### encapsulation {tunnel-mode | transport-mode}

The Encapsulating Security Payload (ESP) encapsulation mode.

- Use `tunnel-mode` to protect the entire inner IP packet, including the inner IP header.
  - Use `transport-mode` to insert ESP after the IP header and before a next layer protocol, e.g. TCP, UDP, ICMP, and so on.
- 

### l2tp {enable | disable}

Enable or disable (by default) L2TP over IPsec.

---

### comments [string]

Optional comments.

---

### protocol <integer>

The quick mode protocol selector. Set the value between 1-255, or 0 (by default) for all.

---

### src-addr-type {subnet | range | ip | name | subnet6 | range6 | ip6 | name6}

**Note:** This entry is only available when `encapsulation` is set to `tunnel-mode`. The local proxy ID type. The default is set to `subnet`. Use `name` to set type to firewall address or group name. Entries with `6` appended to them allow you to set IPv6 options; the other entries allow you to set IPv4 options (see entries below).

---

---

**{src-subnet | src-subnet6} <ip\_netmask>**

**Note:** This entry is only available when `encapsulation` is set to `tunnel-mode`. The entry with 6 appended is only available when `src-addr-type` is set to `subnet6`. The local proxy ID subnet, either IPv4 or IPv6.

---

**src-port <integer>**

The quick mode source port. Set the value between 1-65535, or 0 (by default) for all.

---

**{src-start-ip | src-start-ip6} <start\_ip>**

**Note:** This entry is only available when `src-addr-type` is set to either `range/range6` or `ip/ip6`. The local proxy ID start, either IPv4 or IPv6.

---

**{src-end-ip | src-end-ip6} <end\_ip>**

**Note:** This entry is only available when `src-addr-type` is set to `range`. The local proxy ID end, either IPv4 or IPv6.

---

**{src-name | src-name6} <name>**

**Note:** This entry is only available when `src-addr-type` is set to `name`. The local proxy ID name, either IPv4 or IPv6.

---

**dst-addr-type {subnet | range | ip | name | subnet6 | range6 | ip6 | name6}**

**Note:** This entry is only available when `encapsulation` is set to `tunnel-mode`. The remote proxy ID type. The default is set to `subnet`. Use `name` to set type to firewall address or group name. Entries with 6 appended to them allow you to set IPv6 options; the other entries allow you to set IPv4 options (see entries below).

---

**{dst-subnet | dst-subnet6} <ip\_netmask>**

**Note:** This entry is only available when `encapsulation` is set to `tunnel-mode`. The entry with 6 appended is only available when `dst-addr-type` is set to `subnet6`. The remote proxy ID subnet, either IPv4 or IPv6.

---

**dst-port <integer>**

The quick mode destination port. Set the value between 1-65535, or 0 (by default) for all.

---

**{dst-start-ip | dst-start-ip6} <start\_ip>**

**Note:** This entry is only available when `dst-addr-type` is set to either `range` or `ip`. The remote proxy ID start, either IPv4 or IPv6.

---

**{dst-end-ip | dst-end-ip6} <end\_ip>**

**Note:** This entry is only available when `dst-addr-type` is set to `range`. The remote proxy ID end, either IPv4 or IPv6.

---

**{dst-name | dst-name6} <name>**

**Note:** This entry is only available when `dst-addr-type` is set to `name`. The remote proxy ID name, either IPv4 or IPv6.

## vpn ssl

### ssl settings

Use this command to configure basic SSL VPN settings including idle-timeout values and SSL encryption preferences. If required, you can also enable the use of digital certificates for authenticating remote clients, and specify the IP address of any DNS and/or WINS server that resides on the private network behind the FortiGate unit.

**Note:** SSL VPNs and their commands are only configurable in NAT/Route mode.

#### config authentication-rule

A configuration method to create authentication rules for SSL VPN. Edit to create new and specify the rules using the entries available.

---

**reqclientcert {enable | disable}**

Enable or disable (by default) the requirement of a client certificate. When enabled, the SSL VPN daemon will require a client certificate for all SSL VPN users, regardless of policy.

---

**sslv3 {enable | disable}**

Enable or disable (by default) SSLv3.

SSLv3 is no longer commonly used, and it is recommended to not use this security measure.

---

**tlsv1-0 {enable | disable}**

Enable or disable (by default) Transport Layer Security (TLS) version 1.0 (TLSv1.0).

---

**tlsv1-1 {enable | disable}**

Enable (by default) or disable TLSv1.1.

---

---

**tlsv1-2 {enable | disable}**

Enable (by default) or disable TLSv1.2, currently the most recent version.

---

**banned-cipher <cipher>**

Banned ciphers for SSL VPN. Set one or more of the following to ban the use of cipher suites using:

- **RSA:** Rivest-Shamir-Adleman key
  - **DH:** Diffie Hellman
  - **DHE:** Authenticated ephemeral DH key agreement
  - **ECDH:** Elliptic Curve DH key exchange
  - **ECDHE:** Authenticated ephemeral ECDH key agreement
  - **DSS:** Digital Signature Standard authentication
  - **ECDSA:** Elliptic Curve Digital Signature Algorithm authentication
  - **AES:** Advanced Encryption Standard, either 128 or 256 bit
  - **AESGCM:** AES in Galois Counter Mode
  - **CAMELLIA:** A symmetric block cipher algorithm, either 128 or 256 bit
  - **3DES:** Triple Data Encryption Standard
  - **SHA1:** 160 bit Secure Hash Algorithm
  - **SHA256:** 256 bit SHA
  - **SHA384:** 384 bit SHA
- 

**ssl-big-buffer {enable | disable}**

Enable or disable (by default) big SSLv3 buffer used for communicating with older applications that do not use standard SSL record sizes. When disabled, memory use is reduced by approximately 16kb per connection.

---

**ssl-insert-empty-fragment {enable | disable}**

Enable (by default) or disable the insertion of empty fragments, a counter measure to avoid Browser Exploit Against SSL/TLS (BEAST) attacks.

---

**https-redirect {enable | disable}**

Enable or disable (by default) the redirection of port 80 to the SSL VPN port.

---

**ssl-client-renegotiation {enable | disable}**

Enable (allow) or disable (block, by default) client renegotiation by the server if the tunnel goes down.

---

**force-two-factor-auth {enable | disable}**

Enable or disable (by default) the imposition of two-factor authentication. When enabled, PKI (peer) users will be required to authenticate with their password and certificate authentication. In addition, only PKI users with two-

---

factor authentication enabled will be able to log on to the SSL VPN.

---

### **servercert <cert-name>**

The server's certificate used to identify the FortiGate unit during the SSL handshake with a web browser when the web browser connects to the login page. The certificate must have already been configured on the FortiGate before entering it here. The default is set to `Fortinet_Factory`.

---

### **algorithm {high | medium | low}**

Force the SSL VPN security level. `high` allows only high security algorithms. `medium` allows medium and high. `low` allows any.

---

### **idle-timeout <timeout>**

The period of time in seconds that the SSL VPN will wait before timing out. Set the value between 1-259200 (or 1 second to 3 days), or 0 for no timeout. The default is set to `300`.

---

### **auth-timeout <timeout>**

The period of time in seconds that the SSL VPN will wait before re-authentication is enforced. Set the value between 1-259200 (or 1 second 3 days), or 0 for no timeout. The default is set to `28800`.

---

### **{tunnel-ip-pools | tunnel-ipv6-pools} <pool-name>**

The tunnel IPv4 or IPv6 pools reserved for remote clients. The addresses and address groups must have already been configured on the FortiGate unit before entering them here.

---

### **dns-suffix <string>**

The DNS suffix, with a maximum length of 253 characters.

---

### **{dns-server1 | ipv6-dns-server1} <addr-ip4/6>**

The IPv4 or IPv6 IP address of the primary DNS server that SSL VPN clients will be able to access after a connection has been established. Use the `dns-server2` or `ipv6-dns-server-2` entries to specify a secondary DNS server (see entry below).

---

### **{dns-server2 | ipv6-dns-server2} <addr-ip4/6>**

The IPv4 or IPv6 IP address of the secondary DNS server that SSL VPN clients will be able to access after a connection has been established.

---

---

**{wins-server1 | ipv6-wins-server1} <addr-ip4/6>**

The IPv4 or IPv6 IP address of the primary WINS server that SSL VPN clients will be able to access after a connection has been established. Use the `wins-server2` or `ipv6-wins-server2` entries to specify a secondary WINS server (see entry below).

---

**{wins-server2 | ipv6-wins-server2} <addr-ip4/6>**

The IPv4 or IPv6 IP address of the secondary WINS server that SSL VPN clients will be able to access after a connection has been established.

---

**route-source-interface {enable | disable}**

Enable or disable (by default) allowing SSL VPN connections to bypass routing and bind to the incoming interface.

---

**url-obscuration {enable | disable}**

Enable or disable (by default) encryption of the host name of the URL in the display (web address) of the web browser (for web mode only).

Enabling this feature is required for International Computer Security Association (ICSA) SSL VPN certification. Note that, when enabled, bookmark details are not visible.

---

**http-compression {enable | disable}**

Enable or disable (by default) the use of compression between the FortiGate unit and the client web browser. When enabled, use the `deflate-compression-level` and `deflate-min-data-size` entries to tune performance (see entries below).

---

**http-only-cookie {enable | disable}**

Enable (by default) or disable SSL VPN support for [HttpOnly](#) cookies.

---

**deflate-compression-level <integer>**

**Note:** This entry is only available when `http-compression` is set to `enable`.

The compression level. Set the value between 1-9. Higher compression values reduce the volume of data but requires more processing time. The default is set to 6.

---

**deflate-min-data-size <integer>**

**Note:** This entry is only available when `http-compression` is set to `enable`.

The minimum amount of data in bytes that will trigger compression. Set the value between 200-65535. The default is set to 300.

---



### **port <integer>**

The SSL VPN access port. Set the value between 1-65535. When VDOMs are enabled, this feature is set per VDOM. The default value is set to 10443.

---

### **port-precedence {enable | disable}**

Use this command to control how the FortiGate handles a connection attempt if there is a conflict between administrator access to the GUI and to SSL VPN. This can happen if both SSL VPN and HTTPS admin GUI access use the same port on the same FortiGate interface. When this happens, if `port-precedence` is enabled when an HTTPS connection attempt is received on an interface with an SSL VPN portal the FortiGate assumes its an SSL VPN connection attempt and admin GUI access is not allowed. If `port-precedence` is disabled the FortiGate assumes its an admin GUI access attempt and SSL VPN access is not allowed.

Enabled by default.

---

### **auto-tunnel-static-route {enable | disable}**

Enable (by default) or disable the automatic creation of static routes for the networks that can be accessed through the SSL VPN tunnel. This is only possible if tunnel mode is enabled.

---

### **header-x-forwarded-for {pass | add | remove}**

Action when HTTP x-forwarded-for header to forwarded requests.

- `pass` forwards the same HTTP header.
  - `add` (by default) adds the HTTP header.
  - `remove` removes the HTTP header.
  -
- 

### **source-interface <interface>**

The interface(s) to listen on for SSL clients. You must have already configured the interfaces on the FortiGate unit before entering them here. Enter `any` to match any interface in the virtual domain.

---

### **{source-address | source-address6} [addr-ip4/6]**

An optional feature to specify IPv4 or IPv6 addresses from which users can log in. Leave this entry blank to allow login from any address.

---

### **{source-address-negate | source-address6-negate} {enable | disable}**

Enable or disable {by default} inverting the `source-address` or `source-address6` entries so that it instead specifies IPv4 or IPv6 addresses to not allow.

---

---

### default-portal <portal-name>

The name of the default SSL VPN portal, either one of the defaults (`full-access`, `tunnel-access`, or `web-access`) or a custom portal created on the FortiGate unit.

---

### dtls-tunnel {enable | disable}

Enable (by default) or disable the Datagram Transport Layer Security (DTLS) tunnel, allowing datagram-based applications to communicate in a way that prevents eavesdropping, tampering, or message forgery.

---

### check-referer {enable | disable}

Enable or disable (by default) the verification of referer field in HTTP request header.

---

### http-request-header-timeout <timeout>

The amount of time in seconds before the HTTP connection disconnects if HTTP request header is not complete. Set value between 1-60 (or one second to one minute). The default is set to 20.

---

### http-request-body-timeout <timeout>

The amount of time in seconds before the HTTP connection disconnects if HTTP request body is not complete. Set value between 1-60 (or one second to one minute). The default is set to 30.

---

## ssl web host-check-software

Use this command to define the Windows Firewall software and add your own software requirements to the host check list.

**Note:** Host integrity checking is only possible with client computers running Microsoft Windows platforms.

### config check-item-list

A configuration method to set various check item list variables. Edit to create new and configure settings using the following entries.

---

### action {require | deny}

The course of action taken when the item is found.

- `require`: If the item is found, the client meets the check item condition. This is the default option.
  - `deny`: If the item is found, the client is considered to not meet the check item condition. Use this option if it is necessary to prevent the use of a particular security product.
- 

### type {file | registry | process}

The method used to check for the application.

---

- **file:** Looks for any file that would confirm the presence of the application, not just the application's executable file. This is the default option.  
Once set, use the `target` entry below and set it to the full path to the file. Where applicable, you can use environment variables enclosed in percent (%) marks, e.g.  
`%ProgramFiles%\Fortinet\FortiClient\FortiClient.exe.`
- **registry:** Looks for a Windows Registry entry. Once set, use the `target` entry below and set it to the registry item, e.g. `HKLM\SOFTWARE\Fortinet\FortiClient\Misc.`
- **process:** Looks for the application as a running process. Once set, use the `target` entry below and set it to the application's executable file name.

---

### **target <target>**

Depending on what the `type` entry above is set to, set `target` as follows:

- If `type` is `file`, enter the full path to the file.
- If `type` is `registry`, enter the registry item.
- If `type` is `process`, enter the application's executable file name.

---

### **version <version>**

Enter the application version.

---

### **md5s <md5s>**

If `type` is set to `file` or `process`, this entry can be used to enter one or more known MD5 signatures for the application's executable file. You can use a third-party utility to calculate MD5 signatures or hashes for any file. In addition, you can enter multiple signatures to match multiple versions of the application.

---

### **type {av | fw}**

The software type, antivirus (`av`, set by default) or firewall (`fw`). If the software does both, create two separate entries and assign each entry with a type.

---

### **version <version-number>**

Enter the software version.

---

### **guid <guid-value>**

Enter the globally unique identifier (GUID) for the host check application. The value is a hexadecimal number, usually in the form `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`. Windows uses GUIDs to identify applications in the Windows Registry.

## ssl web portal

Use this command to configure the SSL VPN portal service, allowing you to access network resources through a secure channel using a web browser. Administrators can configure login privileges for users and define which network resources are available to the users, including HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP, and SSH.

The portal configuration determines what the user sees when they log in to the FortiGate. Both the administrator and the user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- **full-access:** Includes all widgets available to the user – Session Information, Connection Tool, Bookmarks, and Tunnel Mode.
- **tunnel-access:** Includes Session Information and Tunnel Mode widgets.
- **web-access:** Includes Session Information and Bookmarks widgets.

### reqclientcert {enable | disable}

Enable or disable (by default) the requirement of a client certificate. When enabled, the SSL VPN daemon will require a client certificate for all SSL VPN users, regardless of policy.

---

### {tunnel-mode | ipv6-tunnel-mode} {enable | disable}

Enable (by default) or disable IPv4 or IPv6 tunnel mode.

---

### ip-mode {range | usrgrp}

**Note:** This entry is only available when `tunnel-mode` is set to `enable`.

How users of this SSL VPN tunnel get IP addresses:

- `range` use the IP addresses available for all SSL VPN users as defined by the [config vpn ssl settings](#) command.
- `user-group` use IP addresses associated with individual users or user groups (usually from external authentication servers (such as RADIUS, LDAP, etc.).

---

### auto-connect {enable | disable}

**Note:** This entry is only available when either `tunnel-mode` or `ipv6-tunnel-mode` is set to `enable`.

Enable or disable (by default) FortiClient automatic connection when the system is up.

---

### keep-alive {enable | disable}

**Note:** This entry is only available when either `tunnel-mode` or `ipv6-tunnel-mode` is set to `enable`.

Enable or disable (by default) the automatic reconnection for FortiClient connections by the client.

---

### save-password {enable | disable}

**Note:** This entry is only available when either `tunnel-mode` or `ipv6-tunnel-mode` is set to `enable`.

Enable or disable (by default) FortiClient saving the user's password.

---

### **{ip-pools | ipv6-pools} <pool-names>**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The names of the IPv4 or IPv6 firewall address objects reserved for SSL VPN tunnel mode clients.

---

### **{split-tunneling | ipv6-split-tunneling} {enable | disable}**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

Enable (by default) or disable IPv4 or IPv6 split tunneling, ensuring that only the traffic for the private network is sent to the SSL VPN gateway.

---

### **{split-tunneling-routing-address | ipv6-split-tunneling-routing-address} <address-name>**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

IPv4 or IPv6 SSL VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access.

---

### **{dns-server1 | ipv6-dns-server1} <addr-ip4/6>**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the primary DNS server that SSL VPN clients will be able to access after a connection has been established. Use the `dns-server2` or `ipv6-dns-server-2` entries to specify a secondary DNS server (see entry below).

---

### **{dns-server2 | ipv6-dns-server2} <addr-ip4/6>**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the secondary DNS server that SSL VPN clients will be able to access after a connection has been established.

---

### **{wins-server1 | ipv6-wins-server1} <addr-ip4/6>**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the primary WINS server that SSL VPN clients will be able to access after a connection has been established. Use the `wins-server2` or `ipv6-wins-server2` entries to specify a secondary WINS server (see entry below).

---

### **{wins-server2 | ipv6-wins-server2}**

**Note:** These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the secondary WINS server that SSL VPN clients will be able to access after a connection has been established.

---

### **web-mode {enable | disable}**

Enable or disable (by default) web mode.

---

### **display-bookmark {enable | disable}**

**Note:** This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web mode bookmark widget.

---

### **user-bookmark {enable | disable}**

**Note:** This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable allowing web portal users to create their own bookmarks.

---

### **user-group-bookmark {enable | disable}**

**Note:** This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable allowing web portal users to create bookmarks for all users in the same user group.

---

### **display-connection-tools {enable | disable}**

**Note:** This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web portal connection tools widget.

---

### **display-history {enable | disable}**

**Note:** This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web portal user login history widget.

---

### **display-status {enable | disable}**

**Note:** This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web portal status widget.

---

### **heading <message>**

The portal heading message.

---

### redir-url <url>

**Note:** This entry is only available when `web-mode` is set to `enable`.

The URL of the web page that enables the FortiGate to display a second HTML page when the web portal home page is displayed. The web server for this URL must reside on the private network behind the FortiGate unit.

---

### theme <colour>

**Note:** This entry is only available when `web-mode` is set to `enable`.

The web portal color scheme: `blue` (by default), `gray`, or `orange`.

---

### custom-lang <language>

**Note:** This entry is only available when `web-mode` is set to `enable`.

Change the display language for this web portal. Select from the following options. The options are named according to the config system `custom-language` command that you can use to customize the content of these language files. By default the content of these language files is provided by Fortinet in the languages listed below.

- `GB2312`: Simplified Chinese (using the Guojia Biaozhun (GB), or 'national standard' in Chinese, is the registered character set of the People's Republic of China used for Simplified Chinese characters.)
  - `big5`: Traditional Chinese (using Big5, or Big-5, is a Chinese character encoding method used in Taiwan, Hong Kong, and Macau for Traditional Chinese characters.)
  - `en`: English (using the English character set (Caribbean).)
  - `euc-kr`: Korean (using the Wxtended Unix Code (EUC) is a character encoding system used for Japanese, Korean, and Simplified Chinese. This featured option is specifically for Korean.)
  - `fr`: French (Using the French character set (Standard).)
  - `pg`: Portuguese (Using the Proto-Germanic (PG), also called Common Germanic, character set.)
  - `sp`: Spanish (using the Spanish character set.)
  - `x-sjis`: Japanese (using the Shift Japanese Industrial Standards (SJIS), is a character encoding method for Japanese.)
- 

### host-check {none | av | fw | av-fw | custom}

The type of host checking to perform on endpoints.

- `none`: Do not perform host checking.
  - `av`: Check for antivirus software recognized by the Windows Security Center.
  - `fw`: Check for firewall software recognized by the Windows Security Center.
  - `av-fw`: Check for both antivirus and firewall software recognized by the Windows Security Center.
  - `custom`: Check for the software defined in the `host-check-policy` entry.
- 

### host-check-interval <seconds>

How often the host check function periodically verifies the host check status of endpoints. Range is 120 to 259200 seconds. Default is 0, which disables periodic host checking. If disabled host checking only happens when the

endpoint initially connects to the SSL VPN. Only available if host-check is enabled.

---

### host-check-policy {<policy> [<policy>...]}

Select one or more host-check policy to perform different types of host checking. You can use this option to add a wide range of host checking options to require endpoints to have a wide range of security software. You can see the complete list of host check policies and add more using the [config vpn ssl host-check-software](#) command.

This option is available when `host-check` is set to `custom`.

---

### limit-user-logins {enable | disable}

Enable or disable (by default) permitting each user one SSL VPN session at a time.

---

### mac-addr-check {enable | disable}

Enable or disable (by default) MAC address host checking.

---

### os-check {enable | disable}

Enable or disable (by default) the FortiGate unit to determine what action to take depending on what operating system the client has.

---

### skip-check-for-unsupported-os {enable | disable}

**Note:** This entry is only available when either `os-check` or `virtual-desktop` is set to `enable`.

Enable (by default) or disable skipping the host check if the client operating system doesn't support it.

---

### skip-check-for-unsupported-browser {enable | disable}

**Note:** This entry is only available when either `os-check` or `virtual-desktop` is set to `enable`.

Enable (by default) or disable skipping the host check if the browser doesn't support it.

---

### virtual-desktop {enable | disable}

Enable or disable (by default) the SSL VPN virtual desktop client application. If enabled on the client, attempted connections via SSL VPN are refused.

---

### virtual-desktop-app-list <name>

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

The name of the application list to apply to the virtual desktop (for more information see the [vpn ssl web virtual-desktop-app-list](#) command).



---

**virtual-desktop-clipboard-share {enable | disable}**

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) sharing of the clipboard with the regular desktop.

---

**virtual-desktop-desktop-switch {enable | disable}**

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) switching between virtual and regular desktop.

---

**virtual-desktop-logout-when-browser-close {enable | disable}**

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) automatic logout from virtual desktop when browser is closed.

---

**virtual-desktop-network-share-access {enable | disable}**

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) network share access from the virtual desktop.

---

**virtual-desktop-printing {enable | disable}**

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) printing from the virtual desktop.

---

**virtual-desktop-removable-media-access {enable | disable}**

**Note:** This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) accessing removable media such as USB drives from the virtual desktop.

---

**ssl web realm**

Use this command to configure SSL VPN realms. Use this command to customize the SSL VPN login page for your users, and also create multiple SSL VPN logins for different user groups.

**Note:** When you edit a realm, the name entered is the URL path used to access the SSL VPN login page (do *not* include `http://`).

**max-concurrent-user <number>**

The maximum number of concurrent users. Set the value between 1-65535, or 0 (by default) for unlimited users.

---

**login-page <content>**

Replacement HTML for the SSL VPN login page.

---

---

### virtual-host [host-name]

The virtual host name for the realm (optional), with a maximum length of 255 characters.

## ssl web user-group-bookmark

Use this command to add bookmarks that will appear on the SSL VPN web portal for all of the users in a user group.

### config bookmarks

A configuration method to configure bookmarks to add to the user group.

---

### apptype {citrix | ftp | portforward | rdp | smb | ssh | telnet | vnc | web}

The identifier of the service to associate with the bookmark.

- `citrix`: Citrix web server interface
  - `ftp`: FTP services
  - `portforward`: port forwarding
  - `rdp`: Windows Terminal services
  - `smb`: SMB/CIFS (Windows file share) services
  - `ssh`: SSH services
  - `telnet`: telnet services
  - `vnc`: VNC services
  - `web`: HTTP/HTTPS services (this is set by default)
- 

### folder <folder>

**Note:** This entry is only available when `apptype` is set to either `ftp` or `smb`.

The folder path.

---

### host <host>

**Note:** This entry is only available when `apptype` is set to either `portforward`, `rdp`, `ssh`, `telnet`, or `vnc`.

The host IP address or FQDN.

---

### listening-port <port-number>

**Note:** This entry is only available when `apptype` is set to `portforward`.

The listening port, set to 0 by default.

---

**remote-port <port-number>**

**Note:** This entry is only available when `apptype` is set to `portforward`.

The remote port, set to 0 by default.

---

**show-status-window {enable | disable}**

**Note:** This entry is only available when `apptype` is set to `portforward`.

Enable or disable (by default) the status window display.

---

**url <url>**

The URL for this bookmark.

---

**description <description>**

The description of the bookmark, with a maximum length of 129 characters.

---

**server-layout {en-us-qwerty | de-de-qwertz | fr-fr-azerty | it-it-qwerty | sv-se-qwerty | failsafe}**

**Note:** This entry is only available when `apptype` is set to `rdp`. Also note that this entry is called `keyboard-layout` in FortiOS 5.2.

The keyboard layout. Select from a number of different layouts.

- `en-us-qwerty`: The American-English QWERTY layout. This is set by default.
  - `de-de-qwertz`: The Deutsch QWERTZ layout.
  - `fr-fr-azerty`: The French AZERTY layout.
  - `it-it-qwerty`: The Italian QWERTY layout.
  - `sv-se-qwerty`: The Swedish QWERTY layout.
  - `failsafe`: Forces all keyboard events to be sent as Unicode.
- 

**security {rdp | nla | tls | any}**

**Note:** This entry is only available when `apptype` is set to `rdp`.

The type of encryption security.

- `rdp`: Standard RDP encryption (set by default)
  - `nla`: Network Level Authentication (NLA)
  - `tls`: TLS encryption
  - `any`: Allow the server to choose the type of security.
-

---

**port <integer>**

**Note:** This entry is only available when `apptype` is set to either `rdp` or `vnc`.

The remote port. Set the value between 1-65535. The default value is set to 3389.

---

**logon-user <name>**

**Note:** This entry is only available when `apptype` is set to `rdp`.

The name of the user.

---

**logon-password <password>**

**Note:** This entry is only available when `apptype` is set to either `rdp` or `vnc`.

The user's password.

---

**sso {disable | static | auto}**

A Single-Sign On (SSO) bookmark that automatically enters the login credentials for the bookmark destination.

- `disable`: This is not an SSO bookmark
  - `static`: This is an SSO bookmark
  - `auto`: Determines whether SSO is used or not automatically
- 

**sso-credential {sslvpn-login | alternative}**

**Note:** This entry is only available when `sso` is set to either `static` or `auto`.

How the user's credentials are submitted.

- `sslvpn-login`: The bookmark enters the user's SSL VPN credentials.
  - `alternative`: Alternative credentials are given, as defined in the `sso-username` and `sso-password` entries (see below).
- 

**sso-username <name>**

**Note:** This entry is only available when `sso-credential` is set to `alternative`.

The user's alternative username.

---

**sso-password <password>**

**Note:** This entry is only available when `sso-credential` is set to `alternative`.

The user's alternative password.

---

## config form-data

**Note:** This configuration option is only available when `sso` is set to `static`.

A configuration method to set form data values. Edit to create new and specify the settings using the entry available. When configuring an entry, as an administrator configuring bookmarks for users, enter `%username%` to represent the user's SSL VPN user name. Enter `%passwd%` to represent the user's password.

## ssl web virtual-desktop-app-list

Use this command to create a list of either allowed or blocked applications which can be used when configuring the virtual desktop.

### action {allow | block}

The action to take for this application control list.

- `allow`: Allows the applications on this list and blocks all others. This is set by default.
- `block`: Blocks the applications on this list and allows all others.

---

## config apps

A configuration method of adding the name of the application(s) to be added to this application control list. This can be any name and does not have to match the official name of the application. Edit to create new and specify the applications.

---

## md5s

A configuration method, within `config apps`, of entering one or more known MD5 signatures for the application's executable file. Separate each signature with a space. You can use a third-party utility to calculate MD5 signatures or hashes for any file. In addition, you can enter multiple signatures to match multiple versions of the application. Edit to create new and specify the signatures.

## wanopt

Use these commands to configure FortiGate WAN optimization.

## wanopt auth-group

Use this command to configure WAN optimization authentication groups, which can be used to support secure tunneling between WAN optimization peers.

## auth-method {cert | psk}

Enter your preferred authentication method:

- Use `cert` (by default) to authenticate using a certificate. Once set, use the `cert` entry to specify the name of the certificate (see below).
  - Use `psk` to authenticate using a pre-shared key. Once set, use the `psk` entry to specify the pre-shared key (see below).
- 

### **cert <name>**

**Note:** This entry is only available when `auth-method` is set to `cert`. Local certificate to be used by the peers in this authentication group. The certificate must have already been installed on the FortiGate before entering it here.

---

### **psk <preshared-key>**

**Note:** This entry is only available when `auth-method` is set to `psk`. Pre-shared key to be used for the authentication group.

---

### **peer-accept {any | defined | one}**

Specify whether the authentication group can be used for `any` peer, only the `defined` peers that have been added to the FortiGate unit, or just `one` specific peer. If you select `one`, use the `peer` entry to add the name of the peer to the authentication group.

---

### **peer**

**Note:** This entry is only available when `peer-accept` is set to `one`. Name of one peer to add to this authentication group. The peer must have already been added to the FortiGate before entering it here.

## **wanopt peer**

Use this command to add WAN optimization peers. This command identifies the other FortiGate units, or peers, that the local FortiGate can form WAN optimization tunnels with. When the remote FortiGate unit connects to the local FortiGate unit to start a WAN optimization tunnel, the remote FortiGate unit local host ID is requested. If the local host ID matches a peer added to the local FortiGate unit, then the local FortiGate unit can accept WAN optimization tunnel from the remote FortiGate unit.

### **ip <ipv4-address>**

IP address of the interface that the remote FortiGate unit will use to connect to the local FortiGate unit — this is usually the interface connected to the WAN.

## wanopt profile

Use this command to configure WAN optimization profiles that work in conjunction with security policies to accept specific traffic. All sessions accepted by a firewall policy, that include a WAN optimization profile, and that match that WAN optimization profile, are processed by WAN optimization. WAN optimization profiles must be added to the FortiGates at each end of the tunnel. To learn more about WAN optimization, including profiles and configuration examples, see [Configuring WAN optimization](#) on our Online Help Portal.

### transparent {enable | disable}

Enable (by default) or disable transparent mode for this profile. When enabled, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. When disabled, the source address of the packets received by servers is changed to the address of the FortiGate interface, so servers appear to receive packets from the FortiGate. Routing on the server network is simpler in this case because client addresses are not involved, however the server won't be able to tell which individual client is sending traffic.

### comments <comments>

Optional comments.

### auth-group <group>

**Note:** Assigning an authentication group is mandatory if `secure-tunnel` has been enabled for the profile. Peer authentication group to be used by this WAN optimization profile. Both client and server FortiGates must add the same authentication group, with both the same names and pre-shared key or certificate.

### config {http | cifs | mapi | ftp | tcp}

Use this configuration method to determine various WAN optimization settings for each protocol. The table below depicts those entries that are available for certain protocols (port numbers are the default values for each protocol):

	http	cifs	mapi	ftp	tcp
byte-caching-opt					✓
prefer-chunking	✓	✓		✓	
port	80	445	135	21	1-65535
ssl	✓				✓

	http	cifs	mapi	ftp	tcp
ssl-port	443				443 990 995 465 993
unknown-http-version	✓				
tunnel-non-http	✓				

### status {enable | disable}

Enable or disable (by default) the profile.

### secure-tunnel {enable | disable}

**Note:** This entry can only be enabled when an authentication group has already been assigned to the profile (see the `auth-group` entry above).

Enable or disable (by default) the use of AES-128bit-CBC SSL to encrypt and secure traffic in the WAN optimization tunnel.

The FortiGates use FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. The secure tunnel uses the same TCP port as a non-secure tunnel (TCP port 7810).

### byte-caching {enable | disable}

Enable (by default, *except* `tcp` which is set to `disable`) or disable WAN optimization byte caching for the traffic accepted by this profile.

Byte caching is a WAN optimization technique that reduces the amount of data that has to be transmitted across a WAN by caching file data to be retrieved later, as required.

### byte-caching-opt {mem-only | mem-disk}

**Note:** This entry is only available when configuring `tcp`.

Byte caching method:

- **mem-only:** Byte caching with memory only (set by default).
- **mem-disk:** Byte caching with memory and disk.

### prefer-chunking {dynamic | fix}

**Note:** This entry is only available when configuring either `http`, `cifs`, or `ftp`.

Data chunking preference:

- **dynamic:** Dynamic data chunking preferred. Use to help detect persistent data chunks in a changed file or in an embedded unknown protocol.
- **fix:** Fixed-size data chunking preferred (set by default).

Note that, while `prefer-chunking` is not available in `tcp` or `mapi`, TCP chunking algorithm will be `dynamic`, so long as `byte-caching-opt` is set to `mem-disk`. MAPI only uses `dynamic`, and thus has no option.

### tunnel-sharing {private | shared | express-shared}

Tunnel sharing mode:



- **private:** Used for profiles that accept aggressive protocols such as HTTP and FTP so as to not share tunnels with less-aggressive protocols (set by default).
- **shared:** Used for profiles that accept non-aggressive and non-interactive protocols.
- **express-shared:** Used for profiles that accept interactive protocols, such as Telnet.

### log-traffic {enable | disable}

Enable (by default) or disable traffic logging.

### port <number>

Port used by each protocol for the profile. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this profile.

Set the value between 1-65535 (default values vary between each protocol; see table above).

### ssl {enable | disable}

**Note:** This entry is only available when configuring either `http` or `tcp`.

Enable or disable (by default) SSL offloading for HTTPS traffic.

If enabled, the profile will be ready to accept SSL-encrypted traffic (HTTPS traffic) because `ssl-port` will become available and is set to 443 by default (see entry below). Also, when enabled, you must add an SSL server for each HTTP server that you want to offload SSL encryption/decryption for by using the `config wanopt ssl-server` command.

### ssl-port <https-ports>

**Note:** This entry is only available when `ssl` is set to `enable`.

Ports used for HTTPS traffic offloading. Set value between 1-65535 (default values vary between each protocol; see table above).

### unknown-http-version {reject | tunnel | best-effort}

**Note:** This entry is only available when configuring `http`.

Action to take when an unknown version of HTTP is encountered. Unknown HTTP sessions are those that don't comply with HTTP 0.9, 1.0, or 1.1.

- **reject:** Rejects requests with unknown HTTP version.
- **tunnel:** Tunnels requests with unknown HTTP version (set by default).
- **best-effort:** Proceeds with best effort.

### tunnel-non-http {enable | disable}

**Note:** This entry is only available when configuring `http`.

Enable to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web-caching. TCP protocol optimization is applied to non-HTTP sessions. Disable (by default) to drop non-HTTP sessions that were otherwise accepted by the profile.

## wanopt settings

Use this command to enable traffic logging for WAN optimization and WAN optimization web-caching sessions.

### host-id <id>

Local host ID/name (set to `default-id` by default). Make sure that the local host ID is also entered in the other FortiGate's peer list.

---

### tunnel-ssl-algorithm {high | medium | low}

Relative strength of encryption accepted for SSL tunnel negotiation:

- **high:** Encryption allows AES and 3DES (set by default).
- **medium:** Encryption allows AES, 3DES, and RC4.
- **low:** Encryption allows AES, 3DES, RC4, and DES.

---

### auto-detect-algorithm {simple | diff-req-req}

Automatic detection algorithms used in tunnel negotiation:

- **simple:** Use the same TCP option value from SYN/SYNACK packets. Backward compatible (set by default).
- **diff-req-req:** Use different TCP option value than in SYN/SYNACK packets to avoid false positive detection.

## wanopt storage

Use this command to determine the maximum size of the byte-caching or web-caching database added to the WAN optimization storage. This is determined by setting the total size and then the percentage to be allotted for web-caching. To view the web-cache and WAN optimization cache storage sizes in megabytes instead (and not as a percentage of the total size allotted for the storage), enter the `get` command. The storage sizes will be displayed: `webcache-storage-size` and `wan-optimization-cache-storage-size`. Note that you must have already configured storage settings using the `config system storage` command before you can configure settings here. All FortiGates with hard disks include a default storage name, such as `Internal`.

### size <mb>

Maximum total size of files within the storage. Set the value between 512-14518 (or 512MB to just over 14.5GB). The default value depends on the partition size.

---

### webcache-storage-percentage <percentage>

Percentage of storage available for web-caching (the rest is used for WAN optimization). Set the value between 0-100. The default value is set to 50.

## wanopt webcache

Use this command to change how the WAN optimization web-cache operates. In most cases the default settings are acceptable, however you may wish to change them to improve performance or optimize the cache for your specific configuration.

### max-object-size <kb>

Maximum cacheable object size in kB. All objects retrieved that are larger than the maximum size are delivered to the client but are not stored in the web cache. Set value between 1-2147483 (or 1kB to just over 2GB). The default value is set to 512000 (or 512MB).

---

### neg-resp-time <minutes>

Period of time in minutes to cache negative responses. The default value is set to 0, meaning no negative responses will be cached.

---

### fresh-factor <percentage>

The fresh factor as a percentage. For cached objects that don't have an expiry time, the web cache periodically checks the server to see if any objects have expired. The higher the fresh factor, the less often the checks occur. Set the value between 0-100. The default value is set to 100.

---

### max-ttl

Maximum time-to-live period in minutes an object can stay in the web cache without checking to see if it has expired on the server. Set the value between 1-5256000. The default value is set to 7200 (or five days).

---

### min-ttl

Minimum time-to-live period in minutes an object can stay in the web cache without checking to see if it has expired on the server. Set the value between 1-5256000. The default value is set to 5.

---

### default-ttl

The default period of time in minutes before an object expires. This only applies to those objects that do not already have an expiry time set by the web server. Set the value between 1-5256000. The default value is set to 1440 (or one day).

---

### ignore-ims {enable | disable}

Enable or disable (by default) the if-modified-since (IMS) header to be ignored. If the time specified by the IMS header in the client's conditional request is greater than the last modified time of the object in the cache, it is likely that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object. Enabling `ignore-ims` overrides this behaviour.

---

### ignore-conditional {enable | disable}

Enable or disable (by default) controlling the behaviour of cache-control header values. HTTP 1.1 provides additional controls to the client over the behaviour of caches concerning the staleness of the object. Depending on various Cache-Control headers, the FortiGate can be forced to consult the OCS before serving the object from the cache. For more information about the behaviour of cache-control header values, see [RFC 2616](#).

---

### ignore-pnc {enable | disable}

Enable or disable (by default) the pragma no-cache (PNC) header to be ignored. Typically, if a client sends an HTTP GET request with a PNC header, a cache must consult the OCS before serving the content. This means the FortiGate always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this, PNC requests can degrade performance and increase server-side bandwidth. Enabling `ignore-pnc` ignores the PNC header from the client request.

---

### ignore-ie-reload {enable | disable}

Enable (by default) or disable the FortiGate to ignore the PNC interpretation of Internet Explorer's Accept: / header. Some versions of Internet Explorer issue Accept: / headers instead of PNC headers when you select **Refresh**. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object. Enabling `ignore-ie-reload` ignores this interpretation.

---

### cache-expired {enable | disable}

Enable or disable (by default) caching of type-1 objects that are already expired upon acquisition. When this setting is enabled, type-1 objects that are already expired at the time of acquisition are cached (if all other conditions make the object cachable). If disabled, expired type-1 objects are considered non-cachable.

---

### cache-cookie {enable | disable}

Enable or disable (by default) the caching of cookies. Typically, it is best to not perform cookie caching, as HTTP responses with cookies contain specific user data.

---

### reval-pnc {enable | disable}

Enable or disable (by default) PNC revalidation to address bandwidth concerns. The PNC header in a client's request can affect the efficiency of the FortiGate unit from a bandwidth gain perspective. If you do not want to completely ignore PNC in client requests (such as when using the `ignore-pnc` entry shown above), you can lower the impact of the PNC by enabling `reval-pnc`.

---

### always-revalidate {enable | disable}

Enable or disable (by default) the revalidation of requested cached objects, which have content on the server, before serving it to the client.

---

### cache-by-default {enable | disable}

Enable or disable (by default) the caching of content that lack explicit caching policies from the server.

---

### host-validate {enable | disable}

Enable or disable (by default) the validation of Host: header with original server IP.

---

### external {enable | disable}

Enable or disable (by default) external cache.

## web-proxy

Use these commands to configure the FortiGate web proxy. You can use the FortiGate web proxy and interface settings to enable explicit HTTP and HTTPS proxying on one or more interfaces. When enabled, the FortiGate unit becomes a web proxy server. All HTTP and HTTPS session received by interfaces with explicit web proxy enabled are intercepted by the explicit web proxy relayed to their destinations.

To use the explicit proxy, users must add the IP address of a FortiGate interface and the explicit proxy port number to the proxy configuration settings of their web browsers.

## web-proxy debug-url

Use this command to configure debug URL addresses.

### url-pattern <string>

URL exemption pattern.

---

### status {enable | disable}

Enable (by default) or disable this URL exemption.

---

### exact {enable | disable}

Enable (by default) or disable match exact path.

## web-proxy explicit

Use this command to enable the explicit web proxy and the TCP port used by the explicit proxy.

### append {outgoing-ip | outgoing-ip6} <ip-addresses>

**Note:** This entry is *not* available in Transparent mode. Append IP addresses (IPv4 or IPv6) that outgoing HTTP requests will leave through. Note that an interface must have this IP address to be configured here.

---

### status {enable | disable}

Enable or disable (by default) the explicit web proxy for HTTP and HTTPS sessions.

---

### ftp-over-http {enable | disable}

Enable or disable (by default) ability to proxy FTP sessions sent from a web browser. Once enabled, use the `ftp-incoming-port` entry to set the port that FTP-over-HTTP requests will be accepted on. Note that the explicit proxy only supports FTP with a web browser, not with a standalone FTP client.

---

### socks {enable | disable}

Enable or disable (by default) the Socket Secure (SOCKS) proxy. Once enabled, use the `socks-incoming-port` entry to set the port number that SOCKS traffic from client web browsers will use to connect to the explicit proxy.

---

### http-incoming-port <port>

Port number that HTTP traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 8080. Note that explicit proxy users must configure their web browser's HTTP proxy settings to use this port.

---

### https-incoming-port <port>

Port number that HTTPS traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP. Note that explicit proxy users must configure their web browser's HTTPS proxy settings to use this port.

---

### ftp-incoming-port <port>

**Note:** This entry is only available when `ftp-over-http` is set to `enable`. Port number that FTP-over-HTTP traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to . Port number that FTP-over-HTTP traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP. Note that explicit proxy users must configure their web browser's FTP proxy settings to use this port.

### socks-incoming-port <port>

**Note:** This entry is only available when `socks` is set to `enable`. Port number that SOCKS traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP.

---

### {incoming-ip | incoming-ip6} <ip-addresses>

**Note:** This entry is *not* available in Transparent mode. IP address (IPv4 or IPv6) of a FortiGate interface that should accept sessions for the explicit web proxy. Use this command to restrict the explicit web proxy to only accepting sessions from one FortiGate interface The destination IP address of explicit web proxy sessions should match this IP address.

---

### {outgoing-ip | outgoing-ip6} <ip-addresses>

**Note:** This entry is *not* available in Transparent mode. IP addresses (IPv4 or IPv6) that outgoing HTTP requests will leave through. Note that an interface must have this IP address to be configured here. Multiple interfaces can be specified. This IP address becomes the source address of web proxy sessions exiting the FortiGate.

---

### ipv6-status {enable | disable}

Enable or disable (by default) IPv6 web proxy functionality. Note that all entries in this command involving IPv6 are only available when `ipv6-status` is set to `enable`.

---

### strict-guest {enable | disable}

Enable or disable (by default) strict guest user check in explicit proxy.

---

---

## pref-dns-results {ipv4 | ipv6}

Either IPv4 (by default) or IPv6 DNS result preference.

---

## unknown-http-version {reject | best-effort}

Action to take when the proxy server handles an unknown HTTP version request or message:

- **reject:** Treats the HTTP traffic as malformed and drops it (set by default; more secure option).
  - **best-effort:** Attempts to handle the HTTP traffic as best as it can.
- 

## realm <name>

Name of the authentication realm used to identify the explicit web proxy. Text string can be up to a maximum of 63 characters. If the realm's name includes spaces, enclose it in quotes. No special characters are permitted; only use alphanumeric characters. When a user authenticates with the explicit proxy the HTTP authentication dialog includes the realm so users can use the realm to identify the explicit web proxy.

---

## sec-default-action {accept | deny}

Determines whether the explicit web proxy accepts or denies (by default) sessions if firewall policies have *not* been added for the explicit web proxy.

---

## https-replacement-message {enable | disable}

Enable (by default) or disable the return of a replacement message for HTTPS requests.

---

## message-upon-server-error {enable | disable}

Enable (by default) or disable the return of a replacement message upon server error detection.

---

## pac-file-server-status {enable | disable}

Enable or disable (by default) Proxy Auto-Configuration (PAC) file server settings.

---

## pac-file-server-port <port>

**Note:** This entry is only available when `pac-file-server-status` is set to `enable`. Port number that PAC traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP. Note that explicit proxy users must configure their web browser's PAC proxy settings to use this port.

---



### pac-file-name <name>

**Note:** This entry is only available when `pac-file-server-status` is set to `enable`. Name of the PAC file. The default is set to `.`. Name of the PAC file. The default is set to `proxy.pac`.

---

### pac-file-data <file>

**Note:** This entry is only available when `pac-file-server-status` is set to `enable`. Contents of the PAC file made available from the explicit proxy server for PAC support. Enclose the PAC file text in quotes. The maximum PAC file size is 8192 bytes. You can also copy the contents of a PAC text file and paste the contents into the CLI, so long as the pasted content is between two quotation marks. You can use any PAC file syntax that is supported by your users's browsers. The FortiGate does not parse the PAC file.

---

### pac-file-url <url>

**Note:** This entry is only available to read when you enter `get`; you *cannot* use this entry to edit the PAC file URL. The URL is made up of the values entered in both `pac-file-server-port` and `pac-file-name` entries. Displays the PAC file URL in the following format: `http://<interface-ip>:<pac-port>/<pac-name>`. By default, `<pac-port>` references the value entered in the `http-incoming-port` entry (see above). However, it will instead reference the value entered in `pac-file-server-port` *if* it is changed from its default value. The `<interface-ip>` component of the URL is the interface of the explicit web proxy. If the explicit web proxy is enabled on multiple interfaces there will be multiple PAC URLs. If you have configured an `incoming-ip` (see entry above) then only one PAC file URL is listed. This URL is to be distributed to PAC users.

---

### ssl-algorithm {high | medium | low}

Relative strength of encryption accepted for deep scan:

- **high:** Encryption allows AES and 3DES.
- **medium:** Encryption allows AES, 3DES, and RC4.
- **low:** Encryption allows AES, 3DES, RC4, and DES (set by default).

## web-proxy forward-server

Use this command to support explicit web proxy forwarding, also known as proxy chaining.

### ip <ipv4-address>

**Note:** This entry is only available when `addr-type` is set to `ip`. IP address of the forwarding proxy server.

---

## fqdn <fqdn>

**Note:** This entry is only available when `addr-type` is set to `fqdn`. Fully Qualified Domain Name (FQDN) of the forwarding proxy server.

## addr-type {ip | fqdn}

Address type of the forwarding proxy server: IP (by default) or FQDN.

---

## port <port>

Port number that the forwarding server expects to receive HTTP sessions on. Set the value between 1-65535. The default is set to 3128.

---

## healthcheck {enable | disable}

Enable or disable (by default) proxy server health check, a function that attempts to connect to a web server to make sure that the remote forwarding server is operating. Once enabled, use the `monitor` entry to set the forward health checking URL.

---

## monitor <url>

**Note:** This entry is only available when `health-check` is set to `enable`. URL to use for health check monitoring. If the web proxy can't connect to this URL, it will assume that forwarding server is down. The default is set to `http://www.google.com`.

## server-down-option {block | pass}

Action to take when the forwarding server is down:

- **block:** Blocks sessions until the server comes back up (set by default).
  - **pass:** Allows sessions to connect to their destination.
- 

## comment [string]

Optional comments.

## web-proxy forward-server-group

Use this command to configure a load-balanced group of web proxy forward servers.

## config server-list

A configuration method to determine the load balancing weight for web proxy forwarding servers. **Note:** You can only create entries if a web proxy forwarding server has already been created on the FortiGate. To do so, go to **Network > Explicit Proxy > Web Proxy Forwarding Servers** and select **Create New**.

### weight <weight>

Weight (or ratio) of this server for load balancing. Set the value between 1-100. The default is set to 10.

---

## affinity {enable | disable}

Enable (by default) or disable attaching source-ip's traffic to assigned forward-server until the `forward-server-affinity-timeout` is reached (see [web-proxy global](#)).

## ldb-method {weighted | least-session}

Load-balancing method:

- **weighted:** Distribute to server based on weight (set by default).
  - **least-session:** Distribute to server with lowest session count.
- 

## group-down-option {block | pass}

Action to take if all forward servers are down:

- **block:** Blocks traffic (set by default).
- **pass:** Passes traffic through.

## web-proxy global

Use this command to configure global web proxy settings that control how the web proxy functions and handles web traffic. Typically, you should not have to change the default settings of this command. Also, if your FortiGate is operating with multiple VDOMS, these settings affect all VDOMS.

### proxy-fqdn <fqdn>

FQDN for the proxy for that clients use to connect. The default is set to `default.fqdn`.

---

### max-request-length <kb>

Maximum length in kilobytes (kB) of the HTTP request line. Set the value between 2-64. The default is set to 4.

---

---

### max-message-length <kb>

Maximum length in kB of the HTTP message, not including the body. Set the value between 16-256. The default is set to 32.

---

### strict-web-check {enable | disable}

Enable or disable (by default) the blocking of web sites that send incorrect headers that don't conform to HTTP 1.1 (see [RFC 2616](#) for more information). Enabling this option may block some commonly used websites.

---

### forward-proxy-auth {enable | disable}

Enable or disable (by default) the forwarding of proxy authentication headers. Note that this option is only practical when in explicit mode, because proxy authentication headers are always forwarded when in transparent mode. By default, in explicit mode, proxy authentication headers are blocked by the explicit web proxy. Therefore, enable this entry if you need to allow proxy authentication through the explicit web proxy.

---

### tunnel-non-http {enable | disable}

Enable (by default) or disable the allowance of non-HTTP traffic.

---

### unknown-http-version {reject | tunnel | best-effort}

Action to take when an unknown version of HTTP is encountered. Unknown HTTP sessions are those that don't comply with HTTP 0.9, 1.0, 1.1.

- **reject:** Rejects requests with unknown HTTP version.
- **tunnel:** Tunnels requests with unknown HTTP version.
- **best-effort:** Proceeds with best effort (set by default).

### forward-server-affinity-timeout <minutes>

Period of time in minutes before the source IP's traffic will no longer be assigned to the forward server. Set the value between 6-60 (or six minutes to one hour). The default is set to 30.

---

### max-waf-body-cache-length <kb>

Maximum length in kB of HTTP message processed by the Web Application Firewall (WAF). Set the value between 10-1024 (or 10kB to just over 1MB). The default is set to 100.

---

## webproxy-profile <name>

Web proxy profile name.

## web-proxy profile

Use this command to configure web proxy profiles that control how the web proxy functions and handles web traffic.

### header-client-ip {pass | add | remove}

Action to take on client IP in forwarded requests header. Set the action to one of the following:

- **pass:** Forwards the same HTTP header.
- **add:** Adds the HTTP header.
- **remove:** Removes the HTTP header.

The default is set to `pass`.

---

### header-via-request {pass | add | remove}

Action to take on via-request header in forwarded requests. The default is set to `pass`.

---

### header-via-response {pass | add | remove}

Action to take on via-response header in forwarded requests. The default is set to `pass`.

---

### header-x-forwarded-for {pass | add | remove}

Action to take on X-Forwarded-For (XFF) header in forwarded requests. The default is set to `pass`. XFF is a common non-standard request field, used to identify originating IP addresses of clients, and is also an email-header indicating that an email was forwarded from one or more accounts.

---

### header-front-end-https {pass | add | remove}

Action to take on Front-End-Https header in forwarded requests. The default is set to `pass`. The Front-End-Https header is used for communication between front-end and back-end servers for SSL and formulating URLs using HTTPS instead of HTTP.

---

## config headers

Use this configuration method to define HTTP forwarded requests headers for action.

---

**name <name>**

HTTP forwarded header name.

**action <action>**

Action to take when HTTP header is forwarded:

- **add-to-request:** Add HTTP header to request (set by default).
- **add-to-response:** Add HTTP header to response.
- **remove-from-request:** Remove HTTP header from request.
- **remove-from-response:** Remove HTTP header from response.

**content <content>**

Enter the HTTP header content.

## web-proxy url-match

Use this command to define URLs for forward-matching or cache exemption.

**status {enable | disable}**

Enable (by default) or disable per URL pattern web proxy forwarding and cache exemptions.

---

**url-pattern <string>**

The URL pattern.

---

**forward-server <name>**

Name of the forward server.

---

**cache-exemption {enable | disable}**

Enable or disable (by default) a cache exemption list. When enabled, the specified URL pattern will be exempted from caching.

---

**comment [string]**

Optional comments.

## web-proxy wisp

Use this command to configure web proxy Websense wireless Internet service provider (WISP) servers.

### comment [string]

Optional comments.

---

### outgoing-ip <ip-address>

WISP outgoing IP address.

---

### server-ip <ip-address>

WISP server IP address.

---

### server-port <port>

WISP server port. Set the value between 1-65535. The default is set to 15868.

---

### max-connections <integer>

Maximum number of web proxy WISP connections. Set the value between 4-4096. The default is set to 64.

---

### timeout <seconds>

Period of time in seconds before WISP requests timeout. Set the value between 1-15. The default is set to 5.

## wireless-controller

Use `config wireless-controller` to configure virtual wireless access points that can be associated with multiple physical wireless access points, thereby extending the range of your wireless network.

## wireless-controller ap-status

Use this command to designate detected access points as either accepted, rogue, or rogue APs that are suppressed. To see information about detected access points, use the `get wireless-controller scan` command.

---

**bssid <mac-address>**

The access point's basic service set identifier (BSSID), expressed as the AP's wireless MAC address.

---

**ssid <name>**

The access point's SSID, expressed as the network name for the wireless interface.

---

**status {rogue | accepted | suppressed}**

Status of the AP:

- **rogue:** Defines an AP as undesirable, but still available.
- **accepted:** Defines an AP as accepted in the wireless network.
- **suppressed:** Actively prevents users from connecting to these rogue APs.

If you have rogue APs in your network, you can choose to monitor them. See [Monitoring rogue APs](#) from our Online Help portal for more details.

---

**wireless-controller global**

Use this command to configure global settings for physical access points, also known as WLAN Termination Points (WTPs), configured using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

**name <name>**

Name for the wireless network.

---

**location <location>**

Location of the wireless network.

---

**max-retransmit**

Maximum number of retransmissions for tunnel packet. Set the value between 0-64. The default is set to 3.

---

**data-ethernet-II {enable | disable}**

Enable or disable (by default) the use of Ethernet frame type with 802.3 data tunnel mode.

---



### link-aggregation {enable | disable}

Enable or disable (by default) CAPWAP transmit hash calculation for selecting link aggregation slaves.

---

### mesh-eth-type

Mesh identifier included in packets, especially useful if debugging is required. Set the value between 0-65535. The default is set to 8755.

---

### fiapp-eth-type

Ethernet type for Fortinet Inter-Access Point Protocol (IAPP), or IEEE 802.11F, packets. Set the value between 0-65535. The default is set to 5252.

---

### discovery-mc-addr <multicast-address>

Multicast IP address for AP discovery. The default is set to 244.0.1.140.

---

### max-clients <number>

Maximum number of clients that can connect simultaneously. The default is set to 0, meaning no limitation.

---

### rogue-scan-mac-adjacency

Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection. MAC adjacency can be used to help with rogue detection, as AP WiFi interface MAC addresses are usually in the same range as its wired MAC address. LAN and WiFi network MAC addresses are matched when they are within a defined numerical distance of each other. Set the value between 0-31. The default is set to 7.

---

### ap-log-server {enable | disable}

Enable or disable (by default) the AP log server.

---

### ap-log-server-ip <ip>

AP log server IP address.

---

### ap-log-server-port <port>

AP log server port number.

---

---

## wireless-controller setting

Use this command to configure VDOM-specific options for the wireless controller.

### account-id

FortiCloud customer account ID.

---

### country <country>

Country of operation for your wireless network. This determines the radio channels that are available. Note that you must set the country before you configure access point (WTP) profiles. To display all available countries, enter `set country ?`. The default is set to `US` (United States).

## wireless-controller timers

Use this command to alter global timers for physical access points, also known as WTPs configured using CAPWAP.

### echo-interval

Period of time in seconds before the WTP sends Echo Requests after joining AC. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to `30`.

---

### discovery-interval

Period of time in seconds between discovery requests. Set the value between 2-180 (or two seconds to three minutes). The default is set to `5`.

---

### client-idle-timeout

Period of time in seconds before client is considered idle and timeouts. Set the value between 20-3600 (or 20 seconds to one hour), or `0` for no timeout. The default is set to `300`.

---

### rogue-ap-log

Intervals of time in minutes for periodic logging of rogue APs. Set the value between 0-1440 (or no logging to one day). The default is set to `0`.

---

### fake-ap-log

Intervals of time in minutes for periodic logging of fake APs. Fake APs serve to attract potential hackers and other intruders so as to collect information about them. Set the value between 0-1440 (or no interval to one day). The default is set to 1.

---

### darrp-optimize

Intervals of time in seconds for Dynamic Automatic Radio Resource Provisioning (DARRP) optimization. Set the value between 0-86400 (or no interval to one day). The default is set to 1800.

---

### sta-stats-interval

Intervals of time in seconds between station statistic reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 1.

---

### vap-stats-interval

Intervals of time in seconds between VAP statistic reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 15.

---

### radio-stats-interval

Intervals of time in seconds between radio statistic reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 15.

---

### sta-capability-interval

Intervals of time in seconds between station capability reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 30.

---

### sta-locate-timer

Intervals of time in seconds between station presence flushes by the WTP. Set the value between 0-86400 (or no interval to one day). The default is set to 1800.

---

## wireless-controller vap

Use this command to configure Virtual Access Points (VAPs). The following entries have `append` options, whereby you can add values without needing to retype the whole list of values:

- selected-usergroups
- broadcast-suppression
- rates-11a
- rates-11bg
- rates-11n-ss12
- rates-11n-ss34
- rates-11ac-ss12
- rates-11ac-ss34

### **vdom <name>**

Name of the VLAN ID, if a VLAN will be used.

---

### **fast-roaming {enable | disable}**

Enable (by default) or disable fast-roaming, or pre-authentication, where supported by clients.

---

### **external-fast-roaming {enable | disable}**

Enable or disable (by default) pre-authentication with external non-managed AP.

---

### **mesh-backhaul {enable | disable}**

**Note:** This entry is only available when `security` is set to a WPA type or `open`. Enable or disable (by default) to use this VAP as a WiFi mesh backhaul. WiFi clients cannot connect directly to this SSID.

---

### **max-clients <number>**

Maximum number of clients that can connect simultaneously. The default is set to 0, meaning no limitation.

---

### **max-clients-ap <number>**

Maximum number of clients that can connect simultaneously per AP radio. The default is set to 0, meaning no limitation.

---

### **ssid <name>**

IEEE 802.11 service set identifier, or network name, for the wireless interface. Users who wish to use the wireless network must configure their computers with this network name.

---

### **broadcast-ssid {enable | disable}**

Enable (by default) or disable broadcasting of the SSID. Broadcasting enables clients to connect to the wireless network without first knowing the SSID. For better security, however, it is best to *not* broadcast the SSID.

---

### **security {open | captive-portal | wpa-personal | wpa-personal+captive-portal | wpa-enterprise | wpa2-only-personal | wpa2-only-personal+captive-portal | wpa2-only-enterprise}**

Security mode for the wireless interface. Wireless users must use the same security mode to connect to the same wireless interface.

- **open:** No security; any wireless user can connect to the network (*not* recommended).
  - **captive-portal:** Users are authenticated through a captive web portal.
  - **wpa-personal:** WPA-Personal security, WPA or WPA2.
  - **wpa-personal+captive-portal:** WPA-Personal security, WPA only, with captive portal.
  - **wpa-enterprise:** WPA-Enterprise security, WPA or WPA2.
  - **wpa2-only-personal:** WPA-Personal security, WPA2 only (set by default).
  - **wpa2-only-personal+captive-portal:** WPA-Personal security, WPA2 only, with captive portal.
  - **wpa2-only-enterprise:** WPA-Enterprise security, WPA2 only.
- 

### **pmf {enable | disable}**

Enable or disable (by default) Protected Management Frames (PMF) support. PMF works by adding a Message Integrity Check (MIC) to control packets being sent between a computer and an AP. If a control packet is being spoofed by a malicious device, the MIC check will fail, and discard the frame. This protects users from malicious attackers attempting to exchange encrypted traffic.

---

### **okc {enable | disable}**

Enable or disable Opportunistic Key Caching (OKC) ...

---

### **radius-mac-auth {enable | disable}**

Enable or disable (by default) MAC address authentication of clients. Once enabled, use the `radius-mac-auth-server` entry to specify the server (see entry below).

---

### **radius-mac-auth-server <server>**

**Note:** This entry is only available when `radius-mac-auth` is set to `enable`. RADIUS-based MAC authentication server.

---

---

## auth {radius | usergroup}

---

### portal-message-override-group <name>

**Note:** This entry is only available when `security` is set to a captive portal type. Replacement message group for this VAP. For this entry to be configured, the replacement message must have already been configured using the `config system replacemsg-group` command.

---

### portal-type {auth | auth+disclaimer | disclaimer | email-collect}

**Note:** This entry is only available when `security` is set to a captive portal type. Captive portal type:

- **auth:** A purely authentication portal (set by default).
  - **auth+disclaimer:** Authentication portal with a disclaimer.
  - **disclaimer:** Just a disclaimer.
  - **email-collect:** Portal for email collection.
- 

### selected-usergroups <groups>

**Note:** This entry is only available when `security` is set to a captive portal type. Selective user groups that are permitted to authenticate.

---

### security-exempt-list [name]

**Note:** This entry is only available when `security` is set to a captive portal type. Optional security exempt list for captive portal authentication, as configured under the `config user security-exempt-list` command.

---

### security-redirect-url [url]

**Note:** This entry is only available when `security` is set to a captive portal type. Optional URL for user-redirectation after user passes captive portal authentication.

---

### encrypt {TKIP | AES | TKIP-AES}

**Note:** This entry is only available when `security` is set to a WPA type. Encryption protocol to use:

- **TKIP:** Temporal Key Integrity Protocol, used by the older WPA standard. It is a more secure encryption than WEP, (the original WLAN security protocol), however it too is now deprecated.
- **AES:** Advanced Encryption Standard. This protocol is commonly used with the newer WPA2 standard (set by default).

- **TKIP-AES:** Use both TKIP and AES protocols in order to provide backward compatibility for legacy devices. This option is not recommended, however, as attackers will only need to breach the weaker encryption of the two (TKIP).
- 

### acct-interim-interval <seconds>

---

### passphrase <psk>

**Note:** This entry is only available when `security` is set to a WPA type. Pre-shared key (PSK) for WPA. Set the hexadecimal value between 8-63 characters in length.

---

### intra-vap-privacy {enable | disable}

Enable or disable (by default) blocking of communication between clients of the same AP.

---

### schedule <name>

VAP schedule name.

---

### local-standalone {enable | disable}

Enable or disable (by default) AP local standalone.

---

### local-bridging {enable | disable}

Enable or disable (by default) bridging of wireless and Ethernet interfaces on the FortiAP.

---

### split-tunneling {enable | disable}

Enable or disable (by default) split tunneling. When enabled, split tunneling allows local traffic on the AP to remain local instead of being routed through the WiFi controller.

---

### vlanid <id>

VLAN ID, if a VLAN will be used.

---

---

## dynamic-vlan {enable | disable}

Enable or disable (by default) dynamic VLAN assignment for users based on RADIUS attributes.

---

## multicast-rate <kbps>

Multicast rate in kbps: 0 (set by default), 6000, 12000, or 24000. Higher multicast rates mean that only close, strong signals are allowed. A high device environment will require a higher multicast rate so as to decrease the range between devices and the router.

---

## multicast-enhance {enable | disable}

Enable or disable (by default) conversion of multicast to unicast to improve performance.

---

## broadcast-suppression [suppression-type]

Optional suppression of broadcast message types:

- **dhcp-up:** Uplink DHCP messages
  - **dhcp-down:** Downlink DHCP messages
  - **dhcp-starvation:** DHCP starvation req messages
  - **arp-known:** ARP for known messages
  - **arp-unknown:** ARP for unknown messages
  - **arp-reply:** ARP reply from wireless clients
  - **arp-poison:** ARP poison messages from wireless clients
  - **arp-proxy:** ARP requests for wireless clients as a proxy
  - **netbios-ns:** NetBIOS name services packets with UDP port 137
  - **netbios-ds:** NetBIOS datagram services packets with UDP port 138
  - **ipv6:** IPv6 packets
  - **all-other-mc:** All other multicast messages
  - **all-other-bc:** All other broadcast messages
- 

## me-disable-thresh <subscribers>

Multicast enhancement threshold. Set value between 2-256 subscribers. The default is set to 32.

---

## probe-resp-suppression {enable | disable}

Enable or disable (by default) ignoring of weak signals. When enabled, use the `probe-resp-threshold` entry to define the minimum signal level required for AP response.

---



### probe-resp-threshold <min-level>

**Note:** This entry is only available when `probe-resp-suppression` is set to `enable`. Minimum signal level/threshold in dBm required for AP response to probe requests. Set the value between -95 to -20. The default is set to -80.

### vlan-pooling {wtp-group | disable}

Enable or disable (by default) VLAN pooling, allowing you to group multiple wireless controller VLANs into VLAN pools. These pools are used to load-balance sessions evenly across multiple VLANs. When set to `wtp-group`, VLAN pooling occurs with VLAN assignment by `wtp-group`.

### gtk-rekey {enable | disable}

**Note:** This entry is only available when `security` is set to a WPA type. Enable or disable (by default) WPA re-key interval option. When enabled, use the `gtk-rekey-intv` entry to set the re-key interval time.

### gtk-rekey-intv <interval>

**Note:** This entry is only available when `gtk-rekey` is set to `enable`. WPA re-key interval in seconds. Increase the value for those users who may require a longer time period. Set the value between 1800-864000 (or 30 minutes to 10 days).

### eap-reauth {enable | disable}

### rates-11a <data-rate>

Data rates permitted for 802.11a in Mbps:

<b>6:</b> 6 Mbps supported rate	<b>24:</b> 24 Mbps supported rate
<b>6-basic:</b> 6 Mbps BSS basic rate	<b>24-basic:</b> 24 Mbps BSS basic rate
<b>9:</b> 9 Mbps supported rate	<b>36:</b> 36 Mbps supported rate
<b>9-basic:</b> 9 Mbps BSS basic rate	<b>36-basic:</b> 36 Mbps BSS basic rate
<b>12:</b> 12 Mbps supported rate	<b>48:</b> 48 Mbps supported rate

<b>12-basic:</b> 12 Mbps BSS basic rate	<b>48-basic:</b> 48 Mbps BSS basic rate
<b>18:</b> 18 Mbps supported rate	<b>54:</b> 54 Mbps supported rate
<b>18-basic:</b> 18 Mbps BSS basic rate	<b>54-basic:</b> 54 Mbps BSS basic rate

## rates-11bg <data-rate>

Data rates permitted for 802.11b/g in Mbps:

<b>1:</b> 1 Mbps supported rate	<b>12:</b> 12 Mbps supported rate
<b>1-basic:</b> 1 Mbps BSS basic rate	<b>12-basic:</b> 12 Mbps BSS basic rate
<b>2:</b> 2 Mbps supported rate	<b>18:</b> 18 Mbps supported rate
<b>2-basic:</b> 2 Mbps BSS basic rate	<b>18-basic:</b> 18 Mbps BSS basic rate
<b>5.5:</b> 5.5 Mbps supported rate	<b>24:</b> 24 Mbps supported rate
<b>5.5-basic:</b> 5.5 Mbps BSS basic rate	<b>24-basic:</b> 24 Mbps BSS basic rate
<b>11:</b> 11 Mbps supported rate	<b>36:</b> 36 Mbps supported rate
<b>11-basic:</b> 11 Mbps BSS basic rate	<b>36-basic:</b> 36 Mbps BSS basic rate
<b>6:</b> 6 Mbps supported rate	<b>48:</b> 48 Mbps supported rate
<b>6-basic:</b> 6 Mbps BSS basic rate	<b>48-basic:</b> 48 Mbps BSS basic rate
<b>9:</b> 9 Mbps supported rate	<b>54:</b> 54 Mbps supported rate
<b>9-basic:</b> 9 Mbps BSS basic rate	<b>54-basic:</b> 54 Mbps BSS basic rate

## rates-11n-ss12 <data-rate>

Data rates permitted for 802.11n with 1 or 2 spatial streams:

<b>mcs0/1:</b> MCS index 0 with 1 spatial stream	<b>mcs8/2:</b> MCS index 8 with 1 spatial streams
<b>mcs1/1:</b> MCS index 1 with 1 spatial stream	<b>mcs9/2:</b> MCS index 9 with 1 spatial streams
<b>mcs2/1:</b> MCS index 2 with 1 spatial stream	<b>mcs10/2:</b> MCS index 10 with 2 spatial streams

<b>mcs3/1:</b> MCS index 3 with 1 spatial stream	<b>mcs11/2:</b> MCS index 11 with 2 spatial streams
<b>mcs4/1:</b> MCS index 4 with 1 spatial stream	<b>mcs12/2:</b> MCS index 12 with 2 spatial streams
<b>mcs5/1:</b> MCS index 5 with 1 spatial stream	<b>mcs13/2:</b> MCS index 13 with 2 spatial streams
<b>mcs6/1:</b> MCS index 6 with 1 spatial stream	<b>mcs14/2:</b> MCS index 14 with 2 spatial streams
<b>mcs7/1:</b> MCS index 7 with 1 spatial stream	<b>mcs15/2:</b> MCS index 15 with 2 spatial streams

### rates-11n-ss34 <data-rate>

Data rates permitted for 802.11n with 3 or 4 spatial streams:

<b>mcs16/3:</b> MCS index 16 with 3 spatial streams	<b>mcs24/4:</b> MCS index 24 with 4 spatial streams
<b>mcs17/3:</b> MCS index 17 with 3 spatial streams	<b>mcs25/4:</b> MCS index 25 with 4 spatial streams
<b>mcs18/3:</b> MCS index 18 with 3 spatial streams	<b>mcs26/4:</b> MCS index 26 with 4 spatial streams
<b>mcs19/3:</b> MCS index 19 with 3 spatial streams	<b>mcs27/4:</b> MCS index 27 with 4 spatial streams
<b>mcs20/3:</b> MCS index 20 with 3 spatial streams	<b>mcs28/4:</b> MCS index 28 with 4 spatial streams
<b>mcs21/3:</b> MCS index 21 with 3 spatial streams	<b>mcs29/4:</b> MCS index 29 with 4 spatial streams
<b>mcs22/3:</b> MCS index 22 with 3 spatial streams	<b>mcs30/4:</b> MCS index 30 with 4 spatial streams
<b>mcs23/3:</b> MCS index 23 with 3 spatial streams	<b>mcs31/4:</b> MCS index 31 with 4 spatial streams

### rates-11ac-ss12 <data-rate>

Data rates permitted for 802.11ac with 1 or 2 spatial streams:

<b>mcs0/1:</b> MCS index 0 with 1 spatial stream	<b>mcs0/2:</b> MCS index 0 with 2 spatial streams
<b>mcs1/1:</b> MCS index 1 with 1 spatial stream	<b>mcs1/2:</b> MCS index 2 with 2 spatial streams
<b>mcs2/1:</b> MCS index 2 with 1 spatial stream	<b>mcs2/2:</b> MCS index 2 with 2 spatial streams
<b>mcs3/1:</b> MCS index 3 with 1 spatial stream	<b>mcs3/2:</b> MCS index 3 with 2 spatial streams
<b>mcs4/1:</b> MCS index 4 with 1 spatial stream	<b>mcs4/2:</b> MCS index 4 with 2 spatial streams

<b>mcs5/1:</b> MCS index 5 with 1 spatial stream	<b>mcs5/2:</b> MCS index 5 with 2 spatial streams
<b>mcs6/1:</b> MCS index 6 with 1 spatial stream	<b>mcs6/2:</b> MCS index 6 with 2 spatial streams
<b>mcs7/1:</b> MCS index 7 with 1 spatial stream	<b>mcs7/2:</b> MCS index 7 with 2 spatial streams
<b>mcs8/1:</b> MCS index 8 with 1 spatial stream	<b>mcs8/2:</b> MCS index 8 with 2 spatial streams
<b>mcs9/1:</b> MCS index 9 with 1 spatial stream	<b>mcs9/2:</b> MCS index 9 with 2 spatial streams

## rates-11ac-ss34 <data-rate>

Data rates permitted for 802.11ac with 3 or 4 spatial streams:

<b>mcs0/3:</b> MCS index 0 with 3 spatial streams	<b>mcs0/4:</b> MCS index 0 with 3 spatial streams
<b>mcs1/3:</b> MCS index 1 with 3 spatial streams	<b>mcs1/4:</b> MCS index 1 with 3 spatial streams
<b>mcs2/3:</b> MCS index 2 with 3 spatial streams	<b>mcs2/4:</b> MCS index 2 with 3 spatial streams
<b>mcs3/3:</b> MCS index 3 with 3 spatial streams	<b>mcs3/4:</b> MCS index 3 with 3 spatial streams
<b>mcs4/3:</b> MCS index 4 with 3 spatial streams	<b>mcs4/4:</b> MCS index 4 with 3 spatial streams
<b>mcs5/3:</b> MCS index 5 with 3 spatial streams	<b>mcs5/4:</b> MCS index 5 with 3 spatial streams
<b>mcs6/3:</b> MCS index 6 with 3 spatial streams	<b>mcs6/4:</b> MCS index 6 with 3 spatial streams
<b>mcs7/3:</b> MCS index 7 with 3 spatial streams	<b>mcs7/4:</b> MCS index 7 with 3 spatial streams
<b>mcs8/3:</b> MCS index 8 with 3 spatial streams	<b>mcs8/4:</b> MCS index 8 with 3 spatial streams
<b>mcs9/3:</b> MCS index 9 with 3 spatial streams	<b>mcs9/4:</b> MCS index 9 with 3 spatial streams

## wireless-controller vap-group

Use this command to add multiple SSIDs to VAP groups.

### append vaps <ssid>

Append SSIDs to be included in the VAP group.

**comment [string]**

Optional comments.

---

**vaps <ssids>**

List of SSIDs to be included in the VAP group.

**wireless-controller wids-profile**

Use this command to configured Wireless Intrusion Detection (WIDS) profiles.

**comment [string]**

Optional comments.

---

**ap-scan {enable | disable}**

Enable or disable (by default) rogue AP scanning. Once enabled, configure a series of AP scanning options (see entries below).

---

**ap-bgscan-period <seconds>**

**Note:** This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between background scans. Set the value between 60-3600 (or one minute to one hour). The default is set to 600 (or ten minutes).

---

**ap-bgscan-intv <seconds>**

**Note:** This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between two scanning channels. Set the range between 1-600 (or one seconds to ten minutes). The default is set to 1.

---

**ap-bgscan-duration <milliseconds>**

**Note:** This entry is only available when `ap-scan` is set to `enable`. Listening time in milliseconds on a scanning channel. Set the value between 10-1000. The default is set to 20.

---

---

### ap-bgscan-idle <milliseconds>

**Note:** This entry is only available when `ap-scan` is set to `enable`. Period of idle-time in milliseconds before channel scanning. Set the value between 0-1000. The default is set to 0.

---

### ap-bgscan-report-intv <seconds>

**Note:** This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between background scan reports. Set the value between 15-600 (or 15 seconds to ten minutes). The default is set to 30.

---

### ap-bgscan-disable-day {sunday | monday | tuesday | wednesday | thursday | friday | saturday}

**Note:** This entry is only available when `ap-scan` is set to `enable`. Days of the week when background scanning is *disabled*. By default, no days are set. When this entry is set (to any number of days), use the `ap-bgscan-disable-start` and `ap-bgscan-disable-end` entries to determine start and end times; the period between these two times is when background scanning is disabled.

---

### ap-bgscan-disable-start <hh:mm>

**Note:** This entry is only available when `ap-bgscan-disable-day` is configured. Start time, in the format of hh:mm, for disabling background scanning. The default is set to 00:00.

---

### ap-bgscan-disable-end <hh:mm>

**Note:** This entry is only available when `ap-bgscan-disable-day` is configured. End time, in the format of hh:mm, for disabling background scanning. The default is set to 00:00.

---

### ap-fgscan-report-intv <seconds>

**Note:** This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between foreground scan reports. Set the value between 15-600 (or 15 seconds to ten minutes). The default is set to 15.

---

### ap-scan-passive {enable | disable}

**Note:** This entry is only available when `ap-scan` is set to `enable`. Enable or disable (by default) passive scanning on all channels.

---

### rogue-scan {enable | disable}

**Note:** This entry is only available when `ap-scan` is set to `enable`. Enable or disable (by default) rogue AP on-wire scan.

---

### wireless-bridge {enable | disable}

Enable or disable (by default)

---

### death-broadcast {enable | disable}

Enable or disable (by default) detection of wireless bridge operation, used to raise awareness if your network *doesn't* use a wireless bridge.

---

### null-ssid-probe-resp {enable | disable}

Enable or disable (by default) null SSID probe response detection.

---

### long-duration-attack {enable | disable}

Enable or disable (by default) long-duration attack detection. When enabled, use the `long-duration-thresh` entry to define the threshold.

---

### long-duration-thresh <milliseconds>

Duration of time in milliseconds for long-duration attack detection. Set the value between 1000-32767 (or one second to over 32 seconds). The default is set to 8200 (or just over eight seconds).

---

### invalid-mac-oui {enable | disable}

Enable or disable (by default) detection of spoofed MAC addresses. The first three bytes should indicate a known manufacturer.

---

### weak-wep-iv {enable | disable}

Enable or disable (by default) detection of APs using weak WEP encryption.

---

### auth-frame-flood {enable | disable}

Enable or disable (by default) detection of authentication frame flood attacks.

---

---

### assoc-frame-flood {enable | disable}

Enable or disable (by default) detection of association frame flood attacks.

---

### spoofed-deauth {enable | disable}

Enable or disable (by default) detection of spoofed deauthentication packets.

---

### asleep-attack {enable | disable}

Enable or disable (by default) detection of asleep attacks, attempts to crack Lightweight Extensible Authentication Protocol (LEAP) security. LEAP is a wireless LAN authentication method that allows clients to re-authenticate frequently, giving the client a new WEP key each time. Enable or disable (by default) detection of asleep attacks, attempts to crack Lightweight Extensible Authentication Protocol (LEAP) security. LEAP is a wireless LAN authentication method that allows clients to re-authenticate frequently, giving the client a new WEP key each time.

---

### eapol-start-flood {enable | disable}

Enable or disable (by default) detection of Extensible Authentication Protocol (EAP) over LAN (EAPoL) START flood attacks.

---

### eapol-logoff-flood {enable | disable}

Enable or disable (by default) detection of EAPoL LOGOFF flood attacks.

---

### eapol-succ-flood {enable | disable}

Enable or disable (by default) detection of EAPoL SUCC flood attacks.

---

### eapol-fail-flood {enable | disable}

Enable or disable (by default) detection of EAPoL FAIL flood attacks. When enabled, use the `eapol-fail-intv` entry to define the detection interval.

---

### eapol-fail-thresh <threshold>

**Note:** This entry is only available when `eapol-fail-flood` is set to `enable`. The EAPoL FAIL detection threshold interval. Set the value between 2-100. The default is set to 10.

---



### eapol-fail-intv <seconds>

**Note:** This entry is only available when `eapol-fail-flood` is set to `enable`. Interval of time in seconds between EAP FAIL detection. Set the value between 1-3600 (or one second to one hour). The default is set to 1.

---

### eapol-pre-succ-flood {enable | disable}

Enable or disable (by default) detection of EAPoL premature SUCC flood attacks.

---

### eapol-pre-fail-flood {enable | disable}

Enable or disable (by default) detection of EAPoL premature FAIL flood attacks.

---

### deauth-unknown-src-thresh <seconds>

Threshold value per second to deauthenticate unknown sources for DoS attacks. The default is set to 10. Set to 0 for no limitation.

## wireless-controller wtp

Use this command to configure various wireless transaction protocol (WTP) settings, including VAP override options and physical APs for management by the wireless controller, also known as an Access Controller (AC).

**Note:** Radio 2 settings are only available for FortiAP models with dual radios.

### config {radio-1 | radio-2}

A configuration method to set various override options for Radio 1 and/or Radio 2.

#### override-band {enable | disable}

Enable or disable (by default) the override of a specific AP-mode radio band. When enabled, use the `band` entry to configure the band.

#### band {802.11b | 802.11g | 802.11n | 802.11n,g-only | 802.11g-only | 802.11n-only}

**Note:** This entry is only available when `override-band` is set to `enable`.

Band of AP-mode radio. Note that this entry becomes available at the same time as `channel` does. In order to set the band, `channel` must be empty. To do this, enter `unset channel`. The channel may then be set after the band.

#### override-txpower {enable | disable}

Enable or disable (by default) the override of transmission power. When enabled, use the `auto-power-level` and `power-level` entries to configure further power level options.

### auto-power-level {enable | disable}

**Note:** This entry is only available when `override-txpower` is set to `enable`.

Enable or disable (by default) automatic transmission power adjustment. When enabled, use the `auto-power-high` and `auto-power-low` entries to configure the high and low limitations. When disabled, use the `power-level` entry to configure the power level percentage.

### auto-power-high <dBm>

**Note:** This entry is only available when `override-txpower` is set to `enable` and `auto-power-level` is then set to `enable`.

Automatic transmission power high limit in decibels (dB) of the measured power referenced to one milliwatt (mW), or dBm. Set the value between 10-17. The default is set to 17.

### auto-power-low <dBm>

**Note:** This entry is only available when `override-txpower` is set to `enable` and `auto-power-level` is then set to `enable`.

Automatic transmission power low limit in dBm. Set the value between 1-17. The default is set to 10.

### power-level <percentage>

**Note:** This entry is only available when `override-txpower` is set to `enable` and `auto-power-level` is then set to `disable`.

Radio power level as a percentage; as such, set the value between 0-100. The default is set to 100.

The maximum power level (i.e. 100%) will set to the regulatory maximum for your region, as determined by the country entry under `config wireless-controller setting`.

### override-vaps {enable | disable}

Enable or disable (by default) the override of VAPs. When enabled, use the `vap-all` and `vaps` entries to configure the VAPs carried on the physical AP.

### vap-all {enable | disable}

**Note:** This entry is only available when `override-vaps` is set to `enable`.

Enable or disable (by default) the automatic inheritance of all VAPs. If disabled, you can select specific VAPs by using the `vaps` entry (see below).

### vaps <vaps>

**Note:** This entry is only available when `override-vaps` is set to `enable` and `vap-all` is then set to `disable`.

Specific VAPs carried on this physical AP. Separate each value with a space to add multiple VAPs. Values can also be added using `append`.

**override-channel {enable | disable}**

Enable or disable (by default) the override of channels. When enabled, use the `channel` entry to enter the channels used by the AP.

**channel {1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11}**

**Note:** This entry is only available when either `override-band` or `override-channel` are set to `enable`.

Wireless radio channels to override. Separate each value with a space to add multiple channels. Values can also be added using `append`.

---

**config split-tunneling-acl**

**Note:** This configuration method is only available when `split-tunneling-acl-local-ap-subnet` is set to `enable`.

A configuration method to set various split tunneling access control list (ACL) filter lists.

**dest-ip <ipv4>**

IPv4 destination address to be added to the ACL filter.

---

**config lan**

**Note:** This configuration method is only available when `override-lan` is set to `enable`.

A configuration method to set WTP port mode.

**port-mode {offline | nat-to-wan | bridge-to-wan | bridge-to-ssid}**

LAN port mode:

- **offline:** No port bridging (by default)
  - **nat-to-wan:** Bridge NAT to the incoming WAN interface
  - **bridge-to-wan:** Bridge all LAN ports to the WAN interface
  - **bridge-to-ssid:** Bridge all LAN ports to the SSID
- 

**admin {discovered | disable | enable}**

Enable (by default) or disable the AC to provide service to this WTP, or have the WTP discovered through either discovery or join request messages.

---

**name <name>**

Name for the AP.

---

---

## location <location>

Location of the AP.

---

## wtp-profile <profile>

Name of the WTP profile to apply to this AP, as created under `config wireless-controller wtp-profile`.

---

## wtp-mode {normal | remote}

AP operating mode: `normal` (by default) or `remote`. A tunnel mode SSID can be assigned to an AP in normal mode but not remote mode, while a local-bridge mode SSID can be assigned to an AP in either normal mode or remote mode.

---

## override-led-state {enable | disable}

Enable or disable (by default) the override of LED state. When enabled, use the `led-state` entry to enable or disable use of LEDs on WTP.

---

## led-state {enable | disable}

**Note:** This entry is only available when `override-led-state` is set to `enable`. Enable (by default) or disable the use of LEDs on WTP.

---

## override-ip-fragment {enable | disable}

Enable or disable (by default) the override of IP fragmentation. When enabled, use the `ip-fragment-preventing`, `tun-mtu-uplink`, and `tun-mtu-downlink` entries to configure IP fragmentation settings.

---

## ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}

**Note:** This entry is only available when `override-ip-fragment` is set to `enable`. Method by which IP fragmentation is prevented for CAPWAP tunneled control and data packets:

- **tcp-mss-adjust:** TCP maximum segment adjustment (by default).
  - **icmp-unreachable:** Drop packet and send an Internet Control Message Protocol (ICMP) Destination Unreachable error message.
-

### tun-mtu-uplink <bytes>

**Note:** This entry is only available when `override-ip-fragment` is set to `enable`. Uplink tunnel maximum transmission unit (MTU) in octets (eight-bit bytes). An MTU is the largest size packet or frame that can be sent in a packet. Set the value to either 0 (by default), 576, or 1500.

---

### tun-mtu-downlink <bytes>

**Note:** This entry is only available when `override-ip-fragment` is set to `enable`. Downlink tunnel MTU in octets. Set the value to either 0 (by default), 576, or 1500.

---

### override-split-tunnel {enable | disable}

Enable or disable (by default) to override split-tunneling. When enabled, use the `split-tunneling-acl-local-ap-subnet` entry to enable/disable the configuration of ACL filter lists.

---

### split-tunneling-acl-local-ap-subnet {enable | disable}

**Note:** This entry is only available when `override-split-tunnel` is set to `enable`. Enable or disable (by default) specified destinations to be accessed locally instead of through the WiFi controller. When enabled, the `split-tunneling-acl` configuration method will become available.

---

### override-lan {enable | disable}

Enable or disable (by default) to override the WTP LAN port. When enabled, the `lan` configuration method will become available.

---

### override-allowaccess {enable | disable}

Enable or disable (by default) to override management-access per protocol. When enabled, use the `allowaccess` entry to set the protocols permitted management-access.

---

### allowaccess {telnet | http | https | ssh}

**Note:** This entry is only available when `override-allowaccess` is set to `enable`. Protocols to allow management-access to managed APs: `telnet`, `http`, `https`, and `ssh`. Separate each value with a space to add multiple protocols. Values can also be added using `append`.

---

---

## override-login-passwd-change {enable | disable}

Enable or disable (by default) to override the login-password of managed APs. When enabled, use the `login-passwd-change` entry to determine password-change settings.

---

## login-passwd-change {yes | default | no}

**Note:** This entry is only available when `override-login-passwd-change` is set to `enable`. Login password options:

- **yes:** Change login password of the managed AP
  - **default:** Reset login password to factory default
  - **no:** Do not change login password (by default)
- 

## image-download {enable | disable}

Enable (by default) or disable image download of WTP to the AP. In addition, you can use the following command to import the WTP firmware file from a TFTP server:

```
execute wireless-controller upload-wtp-image tftp <filename> <TFTP server address>
```

---

## mesh-bridge-enable {default | enable | disable}

Enable, disable, or use default (by default) mesh Ethernet bridge local settings on the WTP (when the WTP is configured as a mesh branch-leaf AP).

---

## coordinate-enable {enable | disable}

Enable or disable (by default) AP coordinates. When enabled, use the `coordinate-x` and `coordinate-y` entries to set the AP's X and Y axes.

---

## coordinate-x <string>

**Note:** This entry is only available when `coordinate-enable` is set to `enable`. X axis coordinate of the AP.

---

## coordinate-y <string>

**Note:** This entry is only available when `coordinate-enable` is set to `enable`. Y axis coordinate of the AP.

---

## wireless-controller wtp-group

Use this command to add FortiAP models to WTP groups. A FortiAP can belong to no more than one FortiAP group. FortiAP Groups facilitate the application of FortiAP profiles to large numbers of FortiAPs. Through the VLAN Pool feature, a FortiAP Group can be associated with a VLAN to which WiFi clients will be assigned.

### config wtp-list

A configuration method to add member devices to WTP groups created for the model's platform type. In order to add member devices, you must have already used the `platform-type` entry to add a FortiAP model, as per the example CLI configuration below; a group called **wtp-group-1** is created for a FortiAP-221C device and one member device is added:

```
config wireless-controller wtp-group
  edit wtp-group-1
    set platform-type 221C
    config wtp-list
      edit FP221C3X14019926
    end
  end
end
```

### platform-type {enable | disable}

FortiAP models to define the WTP group platform type.

<b>AP-11N:</b> Default 11n AP	<b>24D:</b> FAP24D
<b>220B:</b> FAP220B/221B	<b>112D:</b> FAP112D
<b>223B:</b> FAP223B	<b>223C:</b> FAP223C
<b>210B:</b> FAP210B	<b>321C:</b> FAP321C
<b>222B:</b> FAP222B	<b>S321C:</b> FAPS321C
<b>112B:</b> FAP112B	<b>S322C:</b> FAPS322C
<b>320B:</b> FAP320B	<b>S323C:</b> FAPS3232C
<b>11C:</b> FAP11C	<b>S311C:</b> FAPS311C
<b>14C:</b> FAP14C	<b>S313C:</b> FAPS313C
<b>28C:</b> FAP28C	<b>S321CR:</b> FAPS321CR
<b>320C:</b> FAP320C	<b>S322CR:</b> FAPS322CR

<b>221C:</b> FAP221C	<b>S323CR:</b> FAPS323CR
<b>25D:</b> FAP25D	<b>S421E:</b> FAPS421E
<b>222C:</b> FAP222C	<b>S422E:</b> FAPS422E
<b>224D:</b> FAP224D	<b>S423E:</b> FAPS423E
<b>214B:</b> FK214B	<b>421E:</b> FAP421E
<b>21D:</b> FAP21D	<b>423E:</b> FAP423E

## wireless-controller wtp-profile

Use this command to configure WTP profiles (or FortiAP Profiles as shown in the GUI), which define radio settings for a particular platform/FortiAP model. FortiAP units contain two radio transceivers, making it possible to provide both 2.4GHz 802.11b/g/n and 5GHz 802.11a/n service from the same AP. The profile also selects which SSIDs the APs will carry.

For example, a FortiAP can be configured to carry all SSIDs on one radio, while the other only carries a specific SSID. The radios can also be used for monitoring, used for the Rogue AP detection feature. See [Monitoring rogue APs](#) from our Online Help portal for more details, and `config wireless-controller wtp-profile` for various AP detection settings.

**Note:** Radio 2 settings are only available for FortiAP models with dual radios.

## config platform

A configuration method to assign the AP hardware type.

### type <platform>

WTP platform type/model. For a full list of options, enter `set type ?` (or see `wireless-controller wtp-group`). The default is set to 220B.

## config deny-mac-list

A configuration methods to deny specific wireless MAC addresses.

### mac <mac-address>

Wireless MAC address to deny.

## config split-tunneling-acl

A configuration method to set various split tunneling access control list (ACL) filter lists.



**dest-ip <ipv4-netmask>**

IPv4 destination address to be added to the ACL filter.

**config {radio-1 | radio-2}**

A configuration method to set various options for Radio 1 and/or Radio 2.

**mode {disabled | ap | monitor | sniffer}**

Radio mode for the AP:

- **disabled:** Radio is not used; *all* other entries are unavailable *except* `powersave-optimize`.
- **ap:** Radio provides wireless AP service (set by default); all other entries are available.
- **monitor:** Radio performs monitoring only; the only other entries available when this is set are `powersave-optimize`, `spectrum-analysis`, and `wids-profile`.
- **sniffer:** Radio performs scanning only; the only other entries available when this is set are `powersave-optimize`, all ap-sniffer related entries, and `spectrum-analysis`.

**band {802.11b | 802.11g | 802.11n | 802.11n,g-only | 802.11g-only | 802.11n-only}**

Band of AP-mode radio. The `n` bands operate at 2.4GHz.

**protection-mode {rtscts | ctsonly | disable}**

**Note:** This entry is only available under `radio-2`. 802.11g protection mode:

- **rtscts:** Enables 802.11g protection in Request to Send/Clear to Send (RTS/CTS) mode, reducing frame collisions
- **ctsonly:** Enables 802.11g protection in CTS mode
- **disable:** Disables 802.11g protection

**powersave-optimize {tim | ac-vo | no-obss-scan | no-11b-rate | client-rate-follow}**

Power-saving optimization options:

- **tim:** Set traffic indication map (TIM) bit for client in power save mode. TIM bit mask indicates to any sleeping listening stations if the AP has any buffered frames present.
- **ac-vo:** Use Access Category (AC) Voice (VO) priority to send packets in the power save queue. AC VO is one of the highest classes/priority levels used to ensure quality of service (QoS).
- **no-obss-scan:** Do not put Overlapping Basic Service Set (OBSS), or high-noise (i.e. non-802.11), scan IE into a Beacon or Probe Response frame.
- **no-11b-rate:** Do not send frame using 11b data rate.
- **client-rate-follow:** Adapt transmitted PHY rate to PHY rate received from client.

Separate each value with a space to add multiple values. Values can also be added using `append`.

**ap-sniffer-bufsize <mb>**

**Note:** This entry is only available when `mode` is set to `sniffer`. AP's sniffer buffer size in MB. Set the value between 1-32. The default is set to 16.

**ap-sniffer-chan <channel>**

**Note:** This entry is only available when `mode` is set to `sniffer`. Channel on which to operate the sniffer. The default is set to 6.

**ap-sniffer-addr <mac-address>**

**Note:** This entry is only available when `mode` is set to `sniffer`. MAC address to monitor.

**ap-sniffer-mgmt-beacon {enable | disable}**

**Note:** This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi management Beacon frame.

**ap-sniffer-mgmt-probe {enable | disable}**

**Note:** This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi management Probe frame.

**ap-sniffer-mgmt-other {enable | disable}**

**Note:** This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi management Other frame.

**ap-sniffer-ctl {enable | disable}**

**Note:** This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi Control frame.

**ap-sniffer-data {enable | disable}**

**Note:** This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi Data frame.

**transmit-optimize {disable | power-save | aggr-limit | retry-limit | send-bar}**

Packet transmission optimization options (enabled by default; all options except `disable`):

- **disable:** No packet transmission optimization
- **power-save:** Tags client as operating in power save mode if excessive transmit retries occur
- **aggr-limit:** Sets a lower aggregation limit when the data rate is low
- **retry-limit:** Sets a lower retry limit when data rate is low
- **send-bar:** Limit transmission of Block Acknowledgement Request (BAR) frames

Separate each value with a space to add multiple values. Values can also be added using `append`.

**amsdu {enable | disable}**

**Note:** This entry is only available under `radio-2`. Enable (by default) or disable Aggregate MAC Service Data Unit (A-MSDU) support, allowing multiple frames to be combined into one larger frame.

### coexistence {enable | disable}

**Note:** This entry is only available under `radio-2`. Enable (by default) or disable HT20/HT40 coexistence support, where bandwidths that use 20MHz and 40MHz can be used in the same channel.

### channel-bonding {40MHz | 20MHz}

**Note:** This entry is only available under `radio-2`. Channel bandwidth: either 40MHz or 20MHz. Channels may use both by enabling the `coexistence` entry (see above).

### auto-power-level {enable | disable}

Enable or disable (by default) automatic power-level adjustment to prevent co-channel interference. When enabled, use the `auto-power-high` and `auto-power-low` entries to configure the high and low limitations. When disabled, use the `power-level` entry to configure the power level percentage.

### auto-power-high <dBm>

**Note:** This entry is only available when `auto-power-level` is set to `enable`. Automatic transmission power high limit in decibels (dB) of the measured power referenced to one milliwatt (mW), or dBm. Set the value between 10-17. The default is set to 17.

### auto-power-low <dBm>

**Note:** This entry is only available when `auto-power-level` is set to `enable`. Automatic transmission power low limit in dBm. Set the value between 1-17. The default is set to 10.

### power-level <percentage>

**Note:** This entry is only available when `auto-power-level` is set to `disable`. Radio power level as a percentage; as such, set the value between 0-100. The default is set to 100. The maximum power level (i.e. 100%) will set to the regulatory maximum for your region, as determined by the country entry under `config wireless-controller setting`.

### dtim <interval>

Interval between an Delivery Traffic Indication Message (DTIM), a kind of TIM that informs clients about the presence of buffered multicast/broadcast data on the AP. Set the value between 1-255. The default is set to 1.

### beacon-interval <milliseconds>

Interval between beacon packets. AP broadcast beacons or TIMs to synchronize wireless networks. Set the value between 40-3500 (or 40 milliseconds to 3.5 seconds). The default is set to 100 (or a tenth of a second). In an environment with high interference, a low `beacon-interval` value might improve network performance. In a location with few wireless nodes, you can increase this value.

### rts-threshold <bytes>

Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS. This will consume more bandwidth, therefore reducing the throughput, however the more RTS packets there are the fewer instances of packet loss will occur. Set the value between 256-2346 (or 256 bytes to over 2kB). The default is set to 2346, meaning that effectively it will never be used, as the maximum packet size in Ethernet networks can only be 1518 bytes (including all headers and maximum data size).

### frag-threshold <bytes>

**Note:** This entry is only available when `band` has been set. Maximum packet size that can be sent without fragmentation. Range is 800 to 2346 bytes. Set the value between 256-2346 (or 256 bytes to over 2kB).

### spectrum-analysis {enable | disable}

Enable or disable (by default) spectrum analysis, a method for finding interference that would negatively impact wireless performance.

### wids-profile

**Note:** This entry is only available when `mode` is set to either `ap` or `monitor`. WIDS profile name to assign to the radio, as configured under the `wireless-controller wids-profile` command.

### darrp {enable | disable}

Enable or disable (by default) Distributed Automatic Radio Resource Provisioning (DARRP), a feature that autonomously and periodically determines the best-suited channel for wireless communication. This allows FortiAP units to select their channel so they do not interfere with each other in large-scale deployments. You can optimize DARRP further under the `wireless-controller timers` command.

### max-clients <integer>

Maximum expected number of STAs supported by the radio. The default is set to 0.

### max-distance <meters>

Maximum expected distance in meters between the AP and clients. This adjusts the ACK timeout to maintain throughput at the maximum distance. Set the value between 0-54000 (or no distance to just over 33.5 miles). The default is set to 0.

### frequency-handoff {enable | disable}

Enable or disable (by default) frequency handoff of clients to other channels. When enabled, you can optimize handoff further by using the `handoff-rssi` and `handoff-sta-thresh` entries.

### ap-handoff {enable | disable}

Enable or disable (by default) handoff of clients to other APs.

### vap-all {enable | disable}

Enable (by default) or disable the automatic inheritance of all VAPs.

### vaps <vaps>

Specific VAPs carried on this physical AP. Separate each value with a space to add multiple VAPs. A maximum of eight VAPs may be added. Values can also be added using `append`.

### channel {1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11}

Wireless radio channels. Separate each value with a space to add multiple channels. Values can also be added using `append`.

## config lbs

A configuration method to set various location based service (LBS) options.

### **ekahau-blink-mode {enable | disable}**

Enable or disable (by default)

### **ekahau-tag <mac-address>**

WiFi frame MAC address.

### **erc-energy-ip <ip-address>**

IP address of the Ekahau real-time location system (RTLS) controller.

### **er-server-port <port>**

Ekahau RTLS controller UDP listening port.

### **aeroscout {enable | disable}**

Enable or disable (by default) AeroScout support.

### **aeroscout-server-ip <ip-address>**

AeroScout server IP address.

### **aeroscout-server-port <port>**

AeroScout server UDP listening port.

### **aeroscout-mu-factor <mu-factor>**

AeroScout Mobile Unit (MU) mode dilution factor. The default is set to 20.

### **aeroscout-mu-timeout <seconds>**

AeroScout MU mode timeout in seconds. Set the value between 0-65535 (or not timeout to over 18 hours). The default is set to 5.

### **fortipresence {enable | disable}**

Enable or disable (by default) FortiPresence support.

### **fortipresence-server <ip-address>**

FortiPresence server IP address.

### **fortipresence-port <port>**

FortiPresence server UDP listening port. Set the value between 300-65535. The default is set to 3000.

**fortipresence-secret <password>**

FortiPresence secret password, with a maximum length of eight characters.

**fortipresence-project <name>**

Name of the FortiPresence project, with a maximum length of 16 characters. The default is set to `fortipresence`.

**fortipresence-frequency <seconds>**

FortiPresence report transmit frequency in seconds. Set the value between 5-65535 (or five seconds to over 18 hours). The default is set to 30.

**fortipresence-rogue {enable | disable}**

Enable or disable (by default) FortiPresence reporting Rogue APs.

**fortipresence-unassoc {enable | disable}**

Enable or disable (by default) FortiPresence reporting unassociated stations.

**station-locate {enable | disable}**

Enable or disable (by default) client station locating services for all clients, whether associated or not.

---

**comment [string]**

Optional comments.

**led-state {enable | disable}**

Enable (by default) or disable

---

**dtls-policy {clear-text | dtls-enabled}**

- clear-text: (set by default).
- dtls-enabled:

Separate each value with a space to add multiple options. Values can also be added using `append`.

---

**max-clients <number>**

The default is set to 0, meaning there is no client limitation.

---

### handoff-rssi <rssi>

Minimum received signal strength indicator (RSSI) value for handoff. Set the value between 20-30. The default is set to 25.

---

### handoff-sta-thresh <threshold>

Threshold value for AP handoff. Set the value between 5-35. The default is set to 30.

---

### handoff-roaming {enable | disable}

Enable (by default) or disable client load balancing during roaming to avoid roaming delay.

---

### ap-country <country>

Country in which this AP will operate. To display all available countries, enter `set country ?`. The default is set to `US` (United States).

---

### ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}

Method by which IP fragmentation is prevented for CAPWAP tunneled control and data packets:

- **tcp-mss-adjust:** TCP maximum segment adjustment (by default).
- **icmp-unreachable:** Drop packet and send an Internet Control Message Protocol (ICMP) Destination Unreachable error message.

Separate with a space to add both values. Values can also be added using `append`.

---

### tun-mtu-uplink <bytes>

Uplink tunnel maximum transmission unit (MTU) in octets (eight-bit bytes). An MTU is the largest size packet or frame that can be sent in a packet. Set the value to either 0 (by default), 576, or 1500.

---

### tun-mtu-downlink <bytes>

Downlink tunnel MTU in octets. Set the value to either 0 (by default), 576, or 1500.

---

### split-tunneling-acl-local-ap-subnet {enable | disable}

Enable or disable (by default) specified destinations to be accessed locally instead of through the WiFi controller.

---

---

## allowaccess {telnet | http | https | ssh}

Protocols to allow management-access to managed APs: `telnet`, `http`, `https`, and `ssh`. Separate each value with a space to add multiple protocols. Values can also be added using `append`.

---

## login-passwd-change {yes | default | no}

Login password options:

- **yes:** Change login password of the managed AP
- **default:** Reset login password to factory default
- **no:** Do not change login password (by default)

When set to `yes`, use the `login-passwd` entry to determine the password of the managed AP.

---

## login-passwd <password>

**Note:** This entry is only available when `login-passwd-change` is set to `yes`. Login password of the managed AP.

---

## lldp {enable | disable}

Enable or disable (by default) Link Layer Discovery Protocol (LLDP), a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbours.



## execute

The execute commands perform immediate operations on the FortiGate unit, including:

- Maintenance operations, such as back up and restore the system configuration, reset the configuration to factory settings, update antivirus and attack definitions, view and delete log messages, set the date and time.
- Network operations, such as view and clear DHCP leases, clear arp table entries, use `ping` or `traceroute` to diagnose network problems.
- Generate certificate requests and install certificates for VPN authentication.

## backup

Back up the FortiGate configuration files, logs, or IPS user-defined signatures file to a TFTP or FTP server, USB disk, or a management station. Management stations can either be a FortiManager unit, or FortiGuard Analysis and Management Service. For more information, see ["fortiguard" on page 1](#) or ["central-management" on page 1](#).

When virtual domain configuration is enabled (in [global](#), `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin can restore the configuration from this file.

When you back up the system configuration from a regular administrator account, the backup file contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

### Syntax

```
execute backup config flash <comment>
execute backup config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config management-station <comment_str>
execute backup config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup config usb <filename_str> [<backup_password_str>]
execute backup config-with-forticlient-info usb-mode [<backup_password_str>]
execute backup config-with-forticlient-info ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config-with-forticlient-info tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup config-with-forticlient-info usb [<backup_password_str>]
execute backup config-with-forticlient-info usb-mode [<backup_password_str>]
execute backup full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup full-config usb <filename_str> [<backup_password_str>]
execute backup full-config usb-mode <filename_str> [<backup_password_str>]
execute backup ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute backup ipsuserdefsig tftp tftp <filename_str> <server_ipv4>
execute backup {disk | memory} alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]
```

```

execute backup {disk | memory} alllogs tftp <server_ipv4>
execute backup {disk | memory} alllogs usb
execute backup {disk | memory} log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_str> <password_str> {traffic | event | ids | virus | webfilter | spam | dlp | voip | app-ctrl | netscan}
execute backup {disk | memory} log tftp <server_ipv4> {traffic | event | ids | virus | webfilter | spam | dlp | voip | app-ctrl | netscan}
execute backup {disk | memory} log usb {traffic | event | ids | virus | webfilter | spam | dlp | voip | app-ctrl | netscan}

```

Variable	Description
config flash <comment>	Back up the system configuration to the flash disk. Optionally, include a comment.
config ftp <filename_str> <server_ipv4[:port_int]   server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to an FTP server.  Optionally, you can specify a password to protect the saved data.
config management-station <comment_str>	Back up the system configuration to a configured management station. If you are adding a comment, do not add spaces, underscore characters (_), or quotation marks (" ") or any other punctuation marks.  The comment you enter displays in both the portal website and FortiGate web-based manager ( <b>System &gt; Maintenance &gt; Revision</b> ).
config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.
config usb <filename_str> [<backup_password_str>]	Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data.
config usb-mode [<backup_password_str>]	Back up the system configuration to a USB disk (Global admin only). Optionally, you can specify a password to protect the saved data.
config-with-forticlient-info ftp <filename_str> <server_ipv4[:port_int]   server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to a file on an FTP server. Optionally, you can specify a password to protect the saved data.
config-with-forticlient-info tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.

Variable	Description
<code>config-with-forticlient-info usb [&lt;backup_password_str&gt;]</code>	Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data.
<code>config-with-forticlient-info usb-mode [&lt;backup_password_str&gt;]</code>	Back up the system configuration to a USB disk (Global admin only). Optionally, you can specify a password to protect the saved data.
<code>full-config ftp &lt;filename_str&gt; &lt;server_ipv4[:port_int]   server_ fqdn[:port_int]&gt; [&lt;username_str&gt; [&lt;password_str&gt;]] [&lt;backup_ password_str&gt;]</code>	Back up the full system configuration to a file on an FTP server. You can optionally specify a password to protect the saved data.
<code>full-config tftp &lt;filename_str&gt; &lt;server_ipv4&gt; [&lt;backup_password_ str&gt;]</code>	Back up the full system configuration to a file on a TFTP server. You can optionally specify a password to protect the saved data.
<code>full-config usb &lt;filename_str&gt; [&lt;backup_password_str&gt;]</code>	Back up the full system configuration to a file on a USB disk. You can optionally specify a password to protect the saved data.
<code>full-config usb-mode &lt;filename_ str&gt; [&lt;backup_password_str&gt;]</code>	Back up the full system configuration to a file on a USB disk (Global admin only). You can optionally specify a password to protect the saved data.
<code>ipsuserdefsig ftp &lt;filename_str&gt; &lt;server_ipv4[:port_int]   server_ fqdn[:port_int]&gt; [&lt;username_str&gt; [&lt;password_str&gt;]]</code>	Backup IPS user-defined signatures to a file on an FTP server.
<code>ipsuserdefsig tftp tftp &lt;filename_ str&gt; &lt;server_ipv4&gt;</code>	Back up IPS user-defined signatures to a file on a TFTP server.
<code>{disk   memory} alllogs ftp &lt;server_ipv4[:port_int]   server_ fqdn[:port_int]&gt; [&lt;username_str&gt; &lt;password_str&gt;]</code>	Back up either all memory or all hard disk log files for this VDOM to an FTP server. The disk option is available on FortiGate models that log to a hard disk.  The file name has the form: <log_file_name>_<VDOM>_<date>_<time>
<code>{disk   memory} alllogs tftp &lt;server_ipv4&gt;</code>	Back up either all memory or all hard disk log files for this VDOM to a TFTP server. The disk option is available on FortiGate models that log to a hard disk.  The file name has the form: <log_file_name>_<VDOM>_<date>_<time>

Variable	Description
<code>{disk   memory} alllogs usb</code>	Back up either all memory or all hard disk log files for this VDOM to a USB disk. The disk option is available on FortiGate models that log to a hard disk. The file name has the form: <code>&lt;log_file_name&gt;_&lt;VDOM&gt;_&lt;date&gt;_&lt;time&gt;</code>
<code>{disk   memory} log ftp &lt;server_ip&gt;[:port_int]   server_fqdn[:port_int] &lt;username_str&gt; &lt;password_str&gt; {traffic   event   ids   virus   webfilter   spam   dlp   voip   app-ctrl   netscan}</code>	Back up the specified type of log file from either hard disk or memory to an FTP server.  The disk option is available on FortiGate models that log to a hard disk.
<code>{disk   memory} log tftp &lt;server_ip&gt; {traffic   event   ids   virus   webfilter   spam   dlp   voip   app-ctrl   netscan}</code>	Back up the specified type of log file from either hard disk or memory to a TFTP server.  The disk option is available on FortiGate models that log to a hard disk.
<code>{disk   memory} log usb {traffic   event   ids   virus   webfilter   spam   dlp   voip   app-ctrl   netscan}</code>	Back up the specified type of log file from either hard disk or memory to a USB disk.  The disk option is available on FortiGate models that log to a hard disk.

## Example

This example shows how to backup the FortiGate unit system configuration to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fgt.cfg 192.168.1.23
```

## batch

Execute a series of CLI commands. `execute batch` commands are controlled by the Maintenance (mntgrp) access control group.

## Syntax

```
execute batch [<cmd_cue>]
```

where `<cmd_cue>` is one of:

`end` — exit session and run the batch commands

`lastlog` — read the result of the last batch commands

`start` — start batch mode

`status` — batch mode status reporting if batch mode is running or stopped

## Example

To start batch mode:

```
execute batch start
Enter batch mode...
```

To enter commands to run in batch mode:

```
config system global
set refresh 5
end
```

To execute the batch commands:

```
execute batch end
Exit and run batch commands...
```

## bypass-mode

Use this command to manually switch a FortiGate-600C or FortiGate-1000C into bypass mode. This is available in transparent mode only. If manually switched to bypass mode, the unit remains in bypass-mode until bypass mode is disabled.

### Syntax

```
execute bypass-mode {enable | disable}
```

## carrier-license

Use this command to enter a FortiOS Carrier license key if you have installed a FortiOS Carrier build on a FortiGate unit and need to enter a license key to enable FortiOS Carrier functionality.

Contact Fortinet Support for more information about this command.

### Syntax

```
execute carrier-license <license_key>
```

Variable	Description
<license_key>	Enter the FortiOS Carrier license key supplied by Fortinet.

## central-mgmt

Update Central Management Service account information. Also used receive configuration file updates from an attached FortiManager unit.

### Syntax

```
execute central-mgmt set-mgmt-id <management_id>
```

```
execute central-mgmt register-device <fmg-serial-number> <fmg-register-password> <fgt-
  user-name> <fgt-password>
execute central-mgmt unregister-device <fmg-serial-number>
```

`set-mgmt-id` is used to change or initially set the management ID, or your account number for Central Management Services. This account ID must be set for the service to be enabled.

`register-device` registers the FortiGate unit with a specific FortiManager unit specified by serial number. You must also specify the administrator name and password that the FortiManager unit uses to log on to the FortiGate unit.

`unregister-device` removes the FortiGate unit from the specified FortiManager unit's device list.

`update` is used to update your Central Management Service contract with your new management account ID. This command is to be used if there are any changes to your management service account.

## Example

If you are registering with the Central Management Service for the first time, and your account number is 123456, you would enter the following:

```
execute central-mgmt set-mgmt-id 123456
```

## cfg reload

Use this command to restore the saved configuration when the configuration change mode is `manual` or `revert`. This command has no effect if the mode is `automatic`, the default. The `set cfg-save` command in `system global` sets the configuration change mode.

When you reload the saved system configuration, the your session ends and the FortiGate unit restarts.

In the default configuration change mode, `automatic`, CLI commands become part of the saved unit configuration when you execute them by entering either `next` or `end`.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. You set the timeout in `system global` using the `set cfg-revert-timeout` command.

## Syntax

```
execute cfg reload
```

## Example

This is sample output from the command when successful:

```
# execute cfg reload
configs reloaded. system will reboot.This is sample output from the command when not in
runtime-only configuration mode:
# execute cfg reload
no config to be reloaded.
```

## cfg save

Use this command to save configuration changes when the configuration change mode is `manual` or `revert`. If the mode is `automatic`, the default, all changes are added to the saved configuration as you make them and this command has no effect. The `set cfg-save` command in `system global` sets the configuration change mode.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are reverted automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. To change the timeout from the default of 600 seconds, go to `system global` and use the `set cfg-revert-timeout` command.

### Syntax

```
execute cfg save
```

### Example

This is sample output from the command:

```
# execute cfg save
config saved.
```

This is sample output when not in runtime-only configuration mode. It also occurs when in runtime-only configuration mode and no changes have been made:

```
# execute cfg save
no config to be saved.
```

## clear system arp table

Clear all the entries in the arp table.

### Syntax

```
execute clear system arp table
```

## cli check-template-status

Reports the status of the secure copy protocol (SCP) script template.

### Syntax

```
execute cli check-template-status
```

## cli status-msg-only

Enable or disable displaying standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session. This command is used for compatibility with FortiManager.

### Syntax

```
execute cli status-msg-only [enable | disable]
```

Variable	Description	Default
status-msg-only [enable   disable]	Enable or disable standardized CLI error output messages. Entering the command without enable or disable disables displaying standardized output.	enable

## client-reputation

Use these commands to retrieve or remove client reputation information.

### Syntax

#### To erase all client reputation data

```
execute client-reputation erase
```

#### To retrieve client reputation host count

```
execute client-reputation host-count <rows>
```

#### To retrieve client reputation host details

```
execute client-reputation host detail <host>
```

#### To retrieve client reputation host summary

```
execute client-reputation host summary <host>
```

#### To purge old data

```
execute client-reputation purge
```

#### To view the top n records

```
execute client-reputation <n | all>
```

## date

Get or set the system date.



## Syntax

```
execute date [<date_str>]
date_str has the form yyyy-mm-dd, where
yyyy is the year and can be 2001 to 2037
mm is the month and can be 01 to 12
dd is the day of the month and can be 01 to 31
```

If you do not specify a date, the command returns the current system date. Shortened values, such as '06' instead of '2006' for the year or '1' instead of '01' for month or day, are not valid.

## Example

This example sets the date to 17 September 2004:

```
execute date 2004-09-17
```

## disk

Use this command to list and format hard disks installed in FortiGate units or individual partitions on these hard disks.

## Syntax

```
execute disk format <partition1_ref_int> [...<partitionn_ref_int>]
execute disk list
execute disk scan <ref_int>
```

Variable	Description
format	Format the referenced disk partitions or disks. Separate reference numbers with spaces.  If you enter a partition reference number the disk partition is formatted. If you enter a disk reference number the entire disk and all of its partitions are formatted.
list	List the disks and partitions and the reference number for each one.
scan	Scan a disk or partition and repair errors.
<ref_int>	Disk (device) or partition reference number.

The `execute disk format` command formats the specified partitions or disks and then reboots the system if a reboot is required.

In most cases you need to format the entire disk only if there is a problem with the partition. Formatting the partition removes all data from the partition. Formatting the disk removes all data from the entire disk and creates a single partition on the disk.

## Examples

Use the following command to list the disks and partitions.

```
execute disk list
```

```
Disk Internal(boot) ref: 14.9GB type: SSD [ATA SanDisk SSD U100] dev: /dev/sda
partition ref: 3 14.4GB, 14.4GB free mounted: Y label: 7464A257123E07BB dev: /dev/sda3
```

In this example, there is only one partition and its reference number is 3.

Enter the following command to format the partition.

```
execute disk format 3
```

After a confirmation message the FortiGate unit formats the partition and restarts. This can take a few minutes.

## disk raid

Use this command to view information about and change the raid settings on FortiGate units that support RAID.

### Syntax

```
execute disk raid disable
execute disk raid enable {Raid-0 | Raid-1 | Raid-5}
execute disk raid rebuild
execute disk raid status
```

Variable	Description
disable	Disable raid for the FortiGate unit.
enable {Raid-0   Raid-1   Raid-5}	Change the RAID level on the FortiGate unit.
rebuild	Rebuild RAID on the FortiGate unit at the same RAID level. You can only execute this command if a RAID error has been detected. Changing the RAID level takes a while and deletes all data on the disk array.
status	Display information about the RAID disk array in the FortiGate unit.

## Examples

Use the following command to display information about the RAID disk array in a FortiGate-82C.

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1000GB

Disk 1: OK Used 1000GB
Disk 2: OK Used 1000GB
Disk 3: OK Used 1000GB
Disk 4: Unavailable Not-Used 0GB
```

## disk scan

Use this command to run a disk check operation.

### Syntax

```
execute disk scan <ref_int>
```

where n is the partition "ref:" number for the disk, shown by `execute disk list`.

The operation requires the FortiGate unit to reboot. The command responds:

### Example

```
# execute disk scan 3
scan requested for: 3/Internal (device=/dev/sda3)
This action requires the unit to reboot.
Do you want to continue? (y/n)
```

## dhcp lease-clear

Clear all DHCP address leases.

### Syntax

For IPv4:

```
execute dhcp lease-clear
```

For IPv6

```
execute dhcp6 lease-clear
```

## dhcp lease-list

Display DHCP leases on a given interface

### Syntax

For IPv4:

```
execute dhcp lease-list [interface_name]
```

For IPv6:

```
execute dhcp6 lease-list [interface_name]
```

If you specify an interface, the command lists only the leases issued on that interface. Otherwise, the list includes all leases issued by DHCP servers on the FortiGate unit.

If there are no DHCP leases in user on the FortiGate unit, an error will be returned.

## disconnect-admin-session

Disconnect an administrator who is logged in.

### Syntax

```
execute disconnect-admin-session <index_number>
```

To determine the index of the administrator that you want to disconnect, view the list of logged-in administrators by using the following command:

```
execute disconnect-admin-session ?
```

The list of logged-in administrators looks like this:

```
Connected:
INDEX  USERNAME  TYPE  FROM  TIME
0      admin    WEB   172.20.120.51  Mon Aug 14 12:57:23 2006
1      admin2   CLI   ssh(172.20.120.54) Mon Aug 14 12:57:23 2006
```

### Example

This example shows how to disconnect the logged administrator `admin2` from the above list.

```
execute disconnect-admin-session 1
```

## enter

Use this command to go from global commands to a specific virtual domain (VDM).

Only available when virtual domains are enabled and you are in config global.

After you enter the VDM, the prompt will not change from “(global)”. However you will be in the VDM with all the commands that are normally available in VDMs.

### Syntax

```
execute enter <vdom>
```

Use “?” to see a list of available VDMs.

## erase-disk

Use this command to reformat the boot device or an attached hard disk. Optionally, this command can restore the image from a TFTP server after erasing.

### Syntax

```
execute erase-disk <disk_name>
```

The <disk\_name> for the boot device is `boot`.

## factoryreset

Reset the FortiGate configuration to factory default settings.

### Syntax

```
execute factoryreset [keepvmlicense]
```

If `keepvmlicense` is specified (VM models only), the VM license is retained after reset.

Apart from the `keepvmlicense` option, this procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses.

## factoryreset2

Reset the FortiGate configuration to factory default settings except VDOM and interface settings.

### Syntax

```
execute factoryreset2 [keepvmlicense]
```

If `keepvmlicense` is specified (VM models only), the VM license is retained after reset.

## formatlogdisk

Format the FortiGate hard disk to enhance performance for logging.

### Syntax

```
execute formatlogdisk
```

---

In addition to deleting logs, this operation will erase all other data on the disk, including system configuration, quarantine files, and databases for antivirus and IPS.

---

## forticarrier-license

Use this command to perform a FortiCarrier license upgrade.

### Syntax

```
execute forticarrier-license <activation-code>
```

## forticlient

Use these commands to manage FortiClient licensing.

## Syntax

### To view FortiClient license information

```
execute forticlient info
```

### To show current FortiClient count

```
execute forticlient list <connection_type>  
where <connection_type> is one of:
```

0 - IPsec

1 - SSLVPN

2 - NAC (Endpoint Security)

3 - WAN optimization

4 - Test

### To upgrade FortiClient licenses

```
execute forticlient upgrade <license_key_str>
```

## FortiClient-NAC

Use the following command to load a FortiClient license onto a FortiGate unit.

## Syntax

```
execute FortiClient-NAC update-registration-license <code>  
where <code> is the FortiClient registration license key/activation code.
```

## fortiguard-log

Use this to manage FortiGuard Analysis and Management Service (FortiCloud) operation.

## Syntax

### To create a FortiCloud account

```
execute fortiguard-log create-account
```

### To perform FortiCloud certification

```
execute fortiguard-log certification
```

### To retrieve the FortiCloud agreement

```
execute fortiguard-log agreement
```

**To test connection to a FortiCloud account**

```
execute fortiguard-log try <account-id> <password>
```

**To join FortiCloud**

```
execute fortiguard-log join
```

**To log in to a FortiCloud account**

```
execute fortiguard-log login <account-id> <password>
```

**To update the FortiGuard Analysis and Management Service contract**

```
execute fortiguard-log update
```

## fortitoken

Use these commands to activate and synchronize a FortiToken device. FortiToken devices are used in two-factor authentication of administrator and user account logons. The device generates a random six-digit code that you enter during the logon process along with user name and password.

Before they can be used to authenticate account logins, FortiToken devices must be activated with the FortiGuard service. When successfully activated, the status of the FortiToken device will change from New to Active.

Synchronization is sometimes needed due to the internal clock drift of the FortiToken device. It is not unusual for new FortiToken units to require synchronization before being put into service. Synchronization is accomplished by entering two sequential codes provided by the FortiToken.

### Syntax

**To activate one or more FortiToken devices**

```
execute fortitoken activate <serial_number> [serial_number2 ... serial_numbern]
```

**To import FortiToken OTP seeds**

```
execute fortitoken import <seeds_file> <seeds_file_preshared_key>
```

**To synchronize a FortiToken device**

```
execute fortitoken sync <serial_number> <code> <next code>
```

**To import a set of FortiToken serial numbers**

```
execute fortitoken import-sn-file <ftk-sn>
```

FortiCare returns a set of 200 serial numbers that are in the same serial number range as the specified FortiToken device.

## fortitoken-mobile

Use these commands to activate and synchronize a FortiToken Mobile card. FortiToken Mobile cards are used in two-factor authentication of administrator and user account logons. The FortiGate unit sends a random six-digit code to the mobile device by email or SMS that the user enters during the logon process along with user name and password.

### Syntax

#### To import the FortiToken Mobile card serial number

```
execute fortitoken-mobile import <activation_code>
```

#### To poll a FortiToken Mobile token state

```
execute fortitoken-mobile poll
```

#### To provision a FortiToken Mobile token

```
execute fortitoken-mobile provision <token_serial_number>
```

## fsso refresh

Use this command to manually refresh user group information from Directory Service servers connected to the FortiGate unit using the Fortinet Single Sign On (FSSO) agent.

### Syntax

```
execute fsso refresh
```

## ha disconnect

Use this command to disconnect a FortiGate unit from a functioning cluster. You must specify the serial number of the unit to be disconnected. You must also specify an interface name and assign an IP address and netmask to this interface of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

To disconnect the unit from the cluster, the `execute ha disconnect` command sets the HA mode of the disconnected unit to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0. The interface specified in the command is set to the IP address and netmask that you specify in the command. In addition all management access to this interface is enabled. Once the FortiGate unit is disconnected you can use SSH, telnet, HTTPS, or HTTP to connect to and manage the FortiGate unit.

### Syntax

```
execute ha disconnect <cluster-member-serial_str> <interface_str> <address_ipv4>  
                    <address_ipv4mask>
```



Variable	Description
cluster-member-serial_str	The serial number of the cluster unit to be disconnected.
interface_str	The name of the interface to configure. The command configures the IP address and netmask for this interface and also enables all management access for this interface.

### Example

This example shows how to disconnect a cluster unit with serial number FGT5002803033050. The internal interface of the disconnected unit is set to IP address 1.1.1.1 and netmask 255.255.255.0.

```
execute ha disconnect FGT5002803033050 internal 1.1.1.1 255.255.255.0
```

## ha ignore-hardware-revision

Use this command to set ignore-hardware-revision status.

### Syntax

#### To view ignore-hardware-revision status

```
execute ha ignore-hardware-revision status
```

#### To set ignore-hardware-revision status

```
execute ha ignore-hardware-revision {enable | disable}
```

## ha manage

Use this command from the CLI of a FortiGate unit in an HA cluster to log into the CLI of another unit in the cluster. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

You can use CLI commands to manage the cluster unit that you have logged into. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.

### Syntax

```
execute ha manage <cluster-index>
```

Variable	Description
cluster-index	<p>The cluster index is assigned by the FortiGate Clustering Protocol according to cluster unit serial number. The cluster unit with the highest serial number has a cluster index of 0. The cluster unit with the second highest serial number has a cluster index of 1 and so on.</p> <p>Enter ? to list the cluster indexes of the cluster units that you can log into. The list does not show the unit that you are already logged into.</p>

## Example

This example shows how to log into a subordinate unit in a cluster of three FortiGate units. In this example you have already logged into the primary unit. The primary unit has serial number FGT3082103000056. The subordinate units have serial numbers FGT3012803021709 and FGT3082103021989.

```
execute ha manage ?
<id>    please input slave cluster index.
<0>     Subsidiary unit FGT3012803021709
<1>     Subsidiary unit FGT3082103021989
```

Type 0 and press enter to connect to the subordinate unit with serial number FGT3012803021709 and log in with a valid administrator account. The CLI prompt changes to the host name of this unit. To return to the primary unit, type `exit`.

From the subordinate unit you can also use the `execute ha manage` command to log into the primary unit or into another subordinate unit. Enter the following command:

```
execute ha manage ?
<id>    please input slave cluster index.
<1>     Subsidiary unit FGT3082103021989
<2>     Subsidiary unit FGT3082103000056
```

Type 2 and press enter to log into the primary unit or type 1 and press enter to log into the other subordinate unit with a valid administrator account. The CLI prompt changes to the host name of this unit.

## ha synchronize

Use this command from a subordinate unit in an HA cluster to manually synchronize its configuration with the primary unit or to stop a synchronization process that is in progress.

### Syntax

```
execute ha synchronize {start | stop}
```

Variable	Description
start	Start synchronizing the cluster configuration.
stop	Stop the cluster from completing synchronizing its configuration.

## interface dhcpclient-renew

Renew the DHCP client for the specified DHCP interface and close the CLI session. If there is no DHCP connection on the specified port, there is no output.

### Syntax

```
execute interface dhcpclient-renew <port>
```

### Example

This is the output for renewing the DHCP client on port1 before the session closes:

```
# execute interface dhcpclient-renew port1
renewing dhcp lease on port1
```

## interface pppoe-reconnect

Reconnect to the PPPoE service on the specified PPPoE interface and close the CLI session. If there is no PPPoE connection on the specified port, there is no output.

### Syntax

```
execute interface pppoe-reconnect <port>
```

## log backup

Use this command to back up all logs, index files, and report databases. The files are compressed and combined into a TAR archive.

### Syntax

```
execute log backup <file name>
where <file name> is the name of the backup file to create.
```

## log client-reputation-report

Use these commands to control client-reputation log actions.

### Syntax

#### To accept a host so that it has its own baselines

```
execute log client-reputation-report accept <policy-id> <host>
```

**To clear all auto-profile data**

```
execute log client-reputation-report clear
```

**To ignore a host, removing it from the abnormal list**

```
execute log client-reputation-report ignore <policy-id> <host>
```

**To refresh the data of one option result**

```
execute log client-reputation-report refresh <policy-id> <option> <action>
```

<option> is one of bandwidth, session, failconn, geo, or app

<action> is one of data, baseline, or data\_baseline (both data and baseline)

**To get baseline/average information of one option**

```
execute log client-reputation-report result baseline <policy-id> <option>
```

<option> is one of bandwidth, session, or failconn

**To get hourly data of a host visiting a country or using an application**

```
execute log client-reputation-report result details {hourly | total} <policy-id>  
    <option> <name> <host>
```

<option> is geo or app

<name> is the name of the country or application

**To list abnormal hosts of one or all options**

```
execute log client-reputation-report result list <policy-id> <option>
```

<option> is geo, app, or all

**To list periodical data of one host of one option**

```
execute log client-reputation-report result period <policy-id> <option> <host>  
    <periods>
```

<option> is one of bandwidth, session, failconn, geo, or app

<periods> is number of periods to list

**To list the top 10 abnormal hosts of one option**

```
execute log client-reputation-report result top10 <policy-id> <option>
```

<option> is one of bandwidth, session, failconn, geo, or app

**To run reports immediately**

```
execute log client-reputation-report run <policy-id>
```

## log convert-oldlogs

Use this command to convert old compact logs to the new format. This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

### Syntax

```
execute log convert-oldlogs
```

## log delete-all

Use this command to clear all log entries for this VDOM in memory and current log files on hard disk. If your FortiGate unit has no hard disk, only log entries in system memory will be cleared. You will be prompted to confirm the command.

### Syntax

```
execute log delete-all
```

## log delete-oldlogs

Use this command to delete old compact logs. This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

### Syntax

```
execute log delete-oldlogs
```

## log detail

Display UTM-related log entries for traffic log entries in this VDOM.

### Syntax

```
execute log detail <category> <utm-ref>
```

where <category> is one of:

- 2: utm-virus
- 3: utm-webfilter
- 4: utm-ips
- 5: utm-spam
- 9: utm-dlp
- 10: utm-app-ctrl

You can obtain <utm-ref> from the `execute log display` output.

## log display

Use this command to display log messages for this VDOM that you have selected with the `execute log filter` command.

### Syntax

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start-line 1
execute log display
```

You can restore the log filters to their default values using the command

```
execute log filter reset
```

## log downgrade-log

Use this command to downgrade existing logs to v5.0 format prior to a firmware downgrade to FortiOS v5.0.

### Syntax

```
execute log downgrade-log
```

## log filter

Use this command to select log messages in this VDOM for viewing or deletion. You can view one log category on one device at a time. Optionally, you can filter the messages to select only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Commands are cumulative. If you omit a required variable, the command displays the current setting.

Use as many `execute log filter` commands as you need to define the log messages that you want to view.

### Syntax

```
execute log filter category <category_name>
execute log filter device {disk | memory}
execute log filter dump
execute log filter field <name> <value> [<value2>,...<valuen>] [not]
execute log filter ha-member <unitsn_str>
execute log filter reset [all | field]
execute log filter rolled_number <number>
execute log filter sortby <field> [max-sort-lines]
execute log filter start-line <line_number>
```

```
execute log filter view-lines <count>
```

Variable	Description	Default
category <category_name>	Enter the type of log you want to select. To see a list of available categories, enter  <code>execute log filter category</code>	event
device {disk   memory}	Device where the logs are stored.	disk
dump	Display current filter settings.	No default.
field <name> <value> [<value2>,...<value n>] [not]	Enter <code>execute log filter field</code> to view the list of field names.  Press Enter after <name> to view information about value parameters for that field.  <code>not</code> inverts the field value condition.	No default.
ha-member <unitsn_str>	Select logs from the specified HA cluster member. Enter the serial number of the unit.	
reset [all   field]	Execute this command to reset all filter settings. You can use field option to reset only filter field settings.	No default.
rolled_number <number>	Select logs from rolled log file. 0 selects current log file.	0
sortby <field> [max-sort-lines]	Sort logs by specified field.	No default.
start-line <line_ number>	Select logs starting at specified line number.	1
view-lines <count>	Set lines per view. Range: 5 to 1000	10

## log fortianalyzer test-connectivity

Use this command to test the connection to the FortiAnalyzer unit. This command is available only when FortiAnalyzer is configured.

### Syntax

```
execute log fortianalyzer test-connectivity
```

### Example

When FortiAnalyzer is connected, the output looks like this:

```
FortiAnalyzer Host Name: FortiAnalyzer-800B
```

```
FortiGate Device ID: FG50B3G06500085
Registration: registered
Connection: allow
Disk Space (Used/Allocated): 468/1003 MB
Total Free Space: 467088 MB
Log: Tx & Rx
Report: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

When FortiAnalyzer is not connected, the output is: `Connect Error`

## log list

You can view the list of current and rolled log files for this VDOM on the console. The list shows the file name, size and timestamp.

### Syntax

```
execute log list <category>
```

To see a list of available categories, enter

```
execute log list
```

### Example

The output looks like this:

```
elog 8704 Fri March 6 14:24:35 2009
elog.1 1536 Thu March 5 18:02:51 2009
elog.2 35840 Wed March 4 22:22:47 2009
```

At the end of the list, the total number of files in the category is displayed. For example:

```
501 event log file(s) found.
```

## log rebuild-sqlldb

Use this command to rebuild the SQL database from log files.

If run in the VDOM context, only this VDOM's SQL database is rebuilt. If run in the global context, the SQL database is rebuilt for all VDOMs.

---

If SQL logging is disabled, this command is unavailable.

---

### Syntax

```
execute log rebuild-sqlldb
```



## log recreate-sqldb

Use this command to recreate SQL log database.

---

If SQL logging is disabled, this command is unavailable.

---

### Syntax

```
execute log recreate-sqldb
```

## log-report reset

Use this command to delete all logs, archives and user configured report templates.

### Syntax

```
execute log-report reset
```

## log restore

Use this command to restore up all logs, index files, and report databases from a backup file created with the "[log backup](#)" on [page 355](#) command.

This command will wipe out all existing logs and report database for the vdom. It is only available for debug firmware builds.

It is recommended to kill reportd and miglogd prior to running this command.

```
kill -3 1
killall miglogd
killall reportd
```

### Syntax

```
execute log restore <file name>
```

where <file name> is the name of the backup file to use.

## log roll

Use this command to roll all log files.

### Syntax

```
execute log roll
```

## log shift-time

Use this command in conjunction with the ["log backup" on page 355](#) and ["log restore" on page 361](#) commands. You can load a log set generated previously to do demos or testing without needing to regenerate data.

### Syntax

```
execute log shift-time <number of hours>
```

## log upload-progress

Use this command to display the progress of the latest log upload.

### Syntax

```
execute log upload-progress
```

## modem dial

Dial the modem.

The dial command dials the accounts configured in `config system modem` until it makes a connection or it has made the maximum configured number of redial attempts.

This command can be used if the modem is in Standalone mode.

### Syntax

```
execute modem dial
```

## modem hangup

Hang up the modem.

This command can be used if the modem is in Standalone mode.

### Syntax

```
execute modem hangup
```

## modem trigger

This command sends a signal to the modem daemon, which causes the state machine to re-evaluate its current state. If for some reason the modem should be connected but isn't, then it will trigger a redial. If the modem should not be connected but is, this command will cause the modem to disconnect.

## Syntax

```
execute modem trigger
```

## mrouter clear

Clear multicast routes, RP-sets, IGMP membership records or routing statistics.

### Syntax

Clear IGMP memberships:

```
execute mrouter clear igmp-group {{<group-address>} <interface-name>}
execute mrouter clear igmp-interface <interface-name>
```

Clear multicast routes:

```
execute mrouter clear <route-type> {<group-address> {<source-address>}}
```

Clear PIM-SM RP-sets learned from the bootstrap router (BSR):

```
execute mrouter clear sparse-mode-bsr
```

Clear statistics:

```
execute mrouter clear statistics {<group-address> {<source-address>}}
```

Variable	Description
<interface-name>	Enter the name of the interface on which you want to clear IGMP memberships.
<group-address>	Optionally enter a group address to limit the command to a particular group.
	Enter one of:
<route-type>	dense-routes - clear only PIM dense routes
	multicast-routes - clear all types of multicast routes
	sparse-routes - clear only sparse routes
<source-address>	Optionally, enter a source address to limit the command to a particular source address. You must also specify group-address.

## netscan

Use this command to start and stop the network vulnerability scanner and perform related functions.

### Syntax

```
execute netscan import
execute netscan list
execute netscan start scan
execute netscan status
```

```
execute netscan stop
```

Variable	Description
import	Import hosts discovered on the last asset discovery scan.
list	List the hosts discovered on the last asset discover scan.
start scan	Start configured vulnerability scan.
status	Display the status of the current network vulnerability scan.
stop	Stop the current network vulnerability scan.

## pbx

Use this command to view active channels and to delete, list or upload music files for when music is playing while a caller is on hold.

### Syntax

```
execute pbx active-call <list>
execute pbx extension <list>
execute pbx ftgd-voice-pkg {sip-trunk}
execute pbx music-on-hold {delete | list | upload}
execute pbx prompt upload ftp <file.tgz> <ftp_server_address>[:port] [<username>]
[password>]
execute pbx prompt upload tftp <file.tgz> <ftp_server_address>[:port] [<username>]
[password>]
execute pbx prompt upload usb <file.tgz> <ftp_server_address>[:port] [<username>]
[password>]
execute pbx restore-default-prompts
execute pbx sip-trunk list
```

Variables	Description
active-call <list>	Enter to display a list of the active calls being processed by the FortiGate Voice unit.
extension <list>	Enter to display the status of all extensions with SIP phones that have connected to the FortiGate Voice unit.
ftgd-voice-pkg {sip-trunk}	Enter to retrieve FortiGuard voice package sip trunk information.
music-on-hold {delete   list   upload}	Enter to either delete, list or upload music on hold files. You can upload music on hold files using FTP, TFTP, or from a USB drive plugged into the FortiGate Voice unit.

Variables	Description
prompt upload ftp <file.tgz> <ftp_ server_address> [:port] [<username> [password>]	Upload new pbx voice prompt files using FTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename, FTP server address (domain name of IPv4 address) and if required the username and password for the server.
prompt upload tftp <file.tgz> <tftp_ server_address> [:port] [<username> [password>]	Upload new pbx voice prompt files using TFTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename and TFTP server IP address.
prompt upload usb <file.tgz> <tftp_ server_address> [:port] [<username> [password>]	Upload new pbx voice prompt files from a USB drive plugged into the FortiGate Voice unit. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename.
restore-default-prompts	Restore default English voicemail and other PBX system prompts. Use this command if you have changed the default prompts and want to restore the default settings.
sip-trunk list	Enter to display the status of all SIP trunks that have been added to the FortiGate Voice configuration.

### Example command output

Enter the following command to view active calls:

```
execute pbx active-call
```

```
Call-From    Call-To    Durationed
6016         6006      00:00:46
```

Enter the following command to display the status of all extensions

```
execute pbx extension list
Extension Host Dialplan
6052 Unregister company-default
6051 Unregister company-default
6050 Unregister company-default
6022 Unregister company-default
6021/6021 172.30.63.34 company-default
6020 Unregister company-default
```

Enter the following command to display the status of all SIP trunks

```
execute pbx sip-trunk list
Name      Host      Username      Account-Type      State
Provider_1 192.169.20.1 +5555555      Static            N/A
```

## ping

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and another network device.

### Syntax

```
execute ping {<address_ipv4> | <host-name_str>}
<host-name_str> should be an IP address, or a fully qualified domain name.
```

### Example

This example shows how to ping a host with the IP address 172.20.120.16.

```
#execute ping 172.20.120.16

PING 172.20.120.16 (172.20.120.16): 56 data bytes
64 bytes from 172.20.120.16: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.20.120.16: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.20.120.16 ping statistics ---
 5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

## ping-options, ping6-options

Set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiGate unit and another network device.

### Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
data-size <bytes>	Specify the datagram size in bytes.	56

Variable	Description	Default
df-bit {yes   no}	Set <code>df-bit</code> to <code>yes</code> to prevent the ICMP packet from being fragmented. Set <code>df-bit</code> to <code>no</code> to allow the ICMP packet to be fragmented.	no
pattern <2-byte_hex>	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the <code>data_size</code> parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default.
repeat-count <repeats>	Specify how many times to repeat ping.	5
source {auto   <source-intf_ip>}	Specify the FortiGate interface from which to send the ping. If you specify <code>auto</code> , the FortiGate unit selects the source address and interface based on the route to the <host-name_str> or <host_ip>. Specifying the IP address of a FortiGate interface tests connections to different network segments from the specified interface.	auto
timeout <seconds>	Specify, in seconds, how long to wait until ping times out.	2
tos <service_type>	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted.  lowdelay = minimize delay throughput = maximize throughput reliability = maximize reliability lowcost = minimize cost	0
ttl <hops>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes   no}	Select <code>yes</code> to validate reply data.	no
view-settings	Display the current ping-option settings.	No default.

## Example

Use the following command to increase the number of pings sent.

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiGate interface with IP address 192.168.10.23.

```
execute ping-options source 192.168.10.23
```

## ping6

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and an IPv6 capable network device.

### Syntax

```
execute ping6 {<address_ipv6> | <host-name_str>}
```

### Example

This example shows how to ping a host with the IPv6 address 12AB:0:0:CD30:123:4567:89AB:CDEF.

```
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

## policy-packet-capture delete-all

Use this command to delete captured packets.

### Syntax

```
execute policy-packet-capture delete-all
```

You will be asked to confirm that you want delete the packets.

## reboot

Restart the FortiGate unit.

---

Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

---

### Syntax

```
execute reboot <comment "comment_string">
```

<comment "comment\_string"> allows you to optionally add a message that will appear in the hard disk log indicating the reason for the reboot. If the message is more than one word it must be enclosed in quotes.

### Example

This example shows the reboot command with a message included.

```
execute reboot comment "December monthly maintenance"
```



## report

Use these commands to manage reports.

### Syntax

#### To flash report caches:

```
execute report flash-cache
```

#### To recreate the report database:

```
execute report recreate-db
```

#### To generate a report:

```
execute report run [<layout_name>["start-time" "end-time"]]
```

The start and end times have the format yyyy-mm-dd hh:mm:ss

## report-config reset

Use this command to reset report templates to the factory default. Logs are not deleted.

---

If SQL logging is disabled, this command is unavailable.

---

### Syntax

```
execute report-config reset
```

## restore

Use this command to

- restore the configuration from a file
- change the FortiGate firmware
- change the FortiGate backup firmware
- restore an IPS custom signature file

When virtual domain configuration is enabled (in `system global`, `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin account can restore the configuration from this file.

A backup file from a regular administrator account contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

## Syntax

```

execute restore av ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore av tftp <filename_str> <server_ipv4[:port_int]>
execute restore config flash <revision>
execute restore config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>] [<backup_password_str>]
execute restore config management-station {normal | template | script} <rev_int>
execute restore config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute restore config usb <filename_str> [<backup_password_str>]
execute restore config usb-mode [<backup_password_str>]
execute restore forticlient tftp <filename_str> <server_ipv4>
execute restore image flash <revision>
execute restore image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
execute restore image usb <filename_str>
execute restore ips ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore ips tftp <filename_str> <server_ipv4>
execute restore ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore ipsuserdefsig tftp <filename_str> <server_ipv4>
execute restore secondary-image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore secondary-image tftp <filename_str> <server_ipv4>
execute restore secondary-image usb <filename_str>
execute restore src-vis <src-vis-pkgfile>
execute restore vcm {ftp | tftp} <filename_str> <server_ipv4>
execute restore vmlicense {ftp | tftp} <filename_str> <server_ipv4>

```

Variable	Description
av ftp <filename_str> <server_ipv4[:port_int]   server_fqdn[:port_int]> [<username_str> <password_str>]	Download the antivirus database file from an FTP server to the FortiGate unit.
av tftp <filename_str> <server_ipv4[:port_int]>	Download the antivirus database file from a TFTP server to the FortiGate unit.
config flash <revision>	Restore the specified revision of the system configuration from the flash disk.

Variable	Description
<pre>config ftp &lt;filename_str&gt; &lt;server_ipv4[:port_ int]   server_fqdn [:port_int]&gt; [&lt;username_str&gt; &lt;password_str&gt;] [&lt;backup_ password_str&gt;]</pre>	<p>Restore the system configuration from an FTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config management- station {normal   template   script} &lt;rev_int&gt;</pre>	<p>Restore the system configuration from the central management server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p><code>rev_int</code> is the revision number of the saved configuration to restore. Enter 0 for the most recent revision.</p>
<pre>config tftp &lt;filename_str&gt; &lt;server_ipv4&gt; [&lt;backup_ password_str&gt;]</pre>	<p>Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config usb &lt;filename_str&gt; [&lt;backup_ password_str&gt;]</pre>	<p>Restore the system configuration from a file on a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config usb-mode [&lt;backup_ password_str&gt;]</pre>	<p>Restore the system configuration from a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords. When the USB drive is removed, the FortiGate unit needs to reboot and revert to the unit's existing configuration.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>forticlient tftp &lt;filename_str&gt; &lt;server_ipv4&gt;</pre>	<p>Download the FortiClient image from a TFTP server to the FortiGate unit. The filename must have the format: <code>FortiClientSetup_versionmajor.versionminor.build.exe</code>. For example, <code>FortiClientSetup.4.0.377.exe</code>.</p>
<pre>image flash &lt;revision&gt;</pre>	<p>Restore specified firmware image from flash disk.</p>

Variable	Description
<pre>image ftp &lt;filename_str&gt; &lt;server_ipv4[:port_ int]   server_fqdn [:port_int]&gt; [&lt;username_str&gt; &lt;password_str&gt;]</pre>	<p>Download a firmware image from an FTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.</p> <p>This command is not available in multiple VDOM mode.</p>
<pre>image management- station &lt;version_ int&gt;</pre>	<p>Download a firmware image from the central management station. This is available if you have configured a FortiManager unit as a central management server. This is also available if your account with FortiGuard Analysis and Management Service allows you to upload firmware images.</p>
<pre>image tftp &lt;filename_str&gt; &lt;server_ipv4&gt;</pre>	<p>Download a firmware image from a TFTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.</p> <p>This command is not available in multiple VDOM mode.</p>
<pre>image usb &lt;filename_str&gt;</pre>	<p>Download a firmware image from a USB disk to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.</p>
<pre>ips ftp &lt;filename_ str&gt; &lt;server_ipv4 [:port_int]   server_ fqdn[:port_int]&gt; [&lt;username_str&gt; &lt;password_str&gt;]</pre>	<p>Download the IPS database file from an FTP server to the FortiGate unit.</p>
<pre>ips tftp &lt;filename_ str&gt; &lt;server_ipv4&gt;</pre>	<p>Download the IPS database file from a TFTP server to the FortiGate unit.</p>
<pre>ipsuserdefsig ftp &lt;filename_str&gt; &lt;server_ipv4[:port_ int]   server_fqdn [:port_int]&gt; [&lt;username_str&gt; &lt;password_str&gt;]</pre>	<p>Restore IPS custom signature file from an FTP server. The file will overwrite the existing IPS custom signature file.</p>
<pre>ipsuserdefsig tftp &lt;filename_str&gt; &lt;server_ipv4&gt;</pre>	<p>Restore an IPS custom signature file from a TFTP server. The file will overwrite the existing IPS custom signature file.</p>

Variable	Description
secondary-image ftp <filename_str> <server_ip4[:port_int]   server_fqdn[:port_int]> [<username_str> <password_str>]	Download a firmware image from an FTP server as the backup firmware of the FortiGate unit. Available on models that support backup firmware images.
secondary-image tftp <filename_str> <server_ip4>	Download a firmware image from a TFTP server as the backup firmware of the FortiGate unit. Available on models that support backup firmware images.
secondary-image usb <filename_str>	Download a firmware image from a USB disk as the backup firmware of the FortiGate unit. The unit restarts when the upload is complete. Available on models that support backup firmware images.
src-vis <src-vis-pkgfile>	Download source visibility signature package.
vcm {ftp   tftp} <filename_str> <server_ip4>	Restore VCM engine/plugin from an ftp or tftp server.
vmlicense {ftp   tftp} <filename_str> <server_ip4>	Restore VM license (VM version of product only).

## Example

This example shows how to upload a configuration file from a TFTP server to the FortiGate unit and restart the FortiGate unit with this configuration. The name of the configuration file on the TFTP server is `backupconfig`. The IP address of the TFTP server is 192.168.1.23.

```
execute restore config tftp backupconfig 192.168.1.23
```

## revision

Use these commands to manage configuration and firmware image files on the local disk.

### Syntax

#### To delete a configuration file

```
execute revision delete config <revision>
```

#### To delete a firmware image file

```
execute revision delete image <revision>
```

**To list the configuration files**

```
execute revision list config
```

**To delete a firmware image file**

```
execute revision list image
```

## router clear bfd session

Use this command to clear bi-directional forwarding session.

**Syntax**

```
execute router clear bfd session <src_ip> <dst_ip> <interface>
```

Variable	Description
<src_ip>	Select the source IP address of the session.
<dst_ip>	Select the destination IP address of the session.
<interface>	Select the interface for the session.

## router clear bgp

Use this command to clear BGP peer connections.

**Syntax**

```
execute router clear bgp all [soft] [in | out]
execute router clear bgp as <as_number> [soft] [in | out]
execute router clear bgp dampening {ip_address | ip/netmask}
execute router clear bgp external {in prefix-filter} [soft] [in | out]
execute router clear bgp flap-statistics {ip_address | ip/netmask}
execute router clear bgp ip <ip_address> [soft] [in | out]
```

Variable	Description
all	Clear all BGP peer connections.
as <as_number>	Clear BGP peer connections by AS number.
dampening {ip_address   ip/netmask}	Clear route flap dampening information for peer or network.
external {in prefix-filter}	Clear all external peers.

Variable	Description
ip <ip_address>	Clear BGP peer connections by IP address.
peer-group	Clear all members of a BGP peer-group.
[in   out]	Optionally limit clear operation to inbound only or outbound only.
flap-statistics {ip_address   ip/netmask}	Clear flap statistics for peer or network.
soft	Do a soft reset that changes the configuration but does not disturb existing sessions.

## router clear ospf process

Use this command to clear and restart the OSPF router.

### Syntax

IPv4:

```
execute router clear ospf process
```

IPv6:

```
execute router clear ospf6 process
```

## router restart

Use this command to restart the routing software.

### Syntax

```
execute router restart
```

## send-fds-statistics

Use this command to send an FDS statistics report now, without waiting for the FDS statistics report interval to expire.

### Syntax

```
execute send-fds-statistics
```

## sensor detail

Use this command to provide information on the FortiGate's hardware components. This command is only supported on select FortiGate models. For example, it does not work on the 100D or the 200D but it does work on the 500D and the 900D.

### Syntax

```
execute sensor detail
```

If you have VDOMs configured on your FortiGate, enter:

```
config global
    execute sensor detail
end
```

### Example

```
# execute sensor detail
1 +3.3V alarm=0 value=3.3342 threshold_status=0
  type=2/1
  upper_non_recoverable=3.6906
  upper_critical=3.6258
  upper_non_critical=3.5124
  lower_non_critical=3.0912
  lower_critical=2.994
  lower_non_recoverable=2.9292
2 +5V alarm=0 value=5.0725 threshold_status=0
  type=2/1
  upper_non_recoverable=5.587
  upper_critical=5.489
  upper_non_critical=5.342
  lower_non_critical=4.6805
  lower_critical=4.5335
  lower_non_recoverable=4.4355
3 +12V alarm=0 value=12.195 threshold_status=0
  type=2/1
  upper_non_recoverable=14.083
  upper_critical=13.729
  upper_non_critical=13.434
  lower_non_critical=10.602
  lower_critical=10.366
  lower_non_recoverable=10.012
. . .
```

## sensor list

Use this command to provide information on the FortiGate's hardware components. This command is only supported on select FortiGate models. For example, it does not work on the 100D or the 200D but it does work on the 500D and the 900D.



## Syntax

```
execute sensor list
```

If you have VDOMs configured on your FortiGate, enter:

```
config global
    execute sensor list
end
```

## Example

```
# execute sensor list
1 +3.3V alarm=0 value=3.2856 threshold_status=0
2 +5V alarm=0 value=5.0235 threshold_status=0
3 +12V alarm=0 value=12.136 threshold_status=0
4 CPU VCCP alarm=0 value=0.9609 threshold_status=0
5 CPU VTT alarm=0 value=1.0589 threshold_status=0
6 CPU PVSA alarm=0 value=0.9315 threshold_status=0
7 P1V8 alarm=0 value=1.7841 threshold_status=0
8 P1V5 alarm=0 value=1.4999 threshold_status=0
9 PCH +1.05V alarm=0 value=1.04 threshold_status=0
10 VCC 2V5 alarm=0 value=2.432 threshold_status=0
11 MAIN 12V alarm=0 value=11.904 threshold_status=0
12 VCC 1V15 alarm=0 value=1.136 threshold_status=0
13 DDR3 VTT alarm=0 value=0.736 threshold_status=0
14 RPS 12V alarm=1 value=0 threshold_status=0x7
15 NCT +3.3V alarm=0 value=3.216 threshold_status=0
16 NCT VBAT alarm=0 value=3.264 threshold_status=0
17 NCT +3.3VSB alarm=0 value=3.216 threshold_status=0
18 NCT VTT alarm=0 value=1.04 threshold_status=0
19 DTS CPU alarm=0 value=50 threshold_status=0
20 CPU Core 0 alarm=0 value=49 threshold_status=0
21 CPU Core 1 alarm=0 value=50 threshold_status=0
22 TD1 alarm=0 value=37 threshold_status=0
23 TD2 alarm=0 value=25 threshold_status=0
24 FAN_TMP_3 alarm=0 value=35 threshold_status=0
25 LM75 U72 alarm=0 value=28 threshold_status=0
26 LM75 U65 alarm=0 value=31 threshold_status=0
27 LM75 U62 alarm=0 value=32 threshold_status=0
28 FAN1 alarm=0 value=4900 threshold_status=0
29 FAN2 alarm=0 value=5000 threshold_status=0
30 FAN3 alarm=0 value=4700 threshold_status=0
```

## set system session filter

Use these commands to define the session filter for `get system session` commands.

### Syntax

#### To clear the filter settings

```
execute set system session filter clear
    {all|dport|dst|duration|expire|policy|proto|sport|src|vd}
```

**To specify destination port**

```
execute set system session filter dport <port_range>
```

**To specify destination IP address**

```
execute set system session filter dst <ip_range>
```

**To specify duration**

```
execute set system session filter duration <duration_range>
```

**To specify expiry**

```
execute set system session filter expire <expire_range>
```

**To list the filter settings**

```
execute set system session filter list
```

**To invert a filter setting**

```
execute set system session filter negate  
{dport|dst|duration|expire|policy|proto|sport|src|vd}
```

**To specify firewall policy ID**

```
execute set system session filter policy <policy_range>
```

**To specify protocol**

```
execute set system session filter proto <protocol_range>
```

**To specify source port**

```
execute set system session filter sport <port_range>
```

**To specify source IP address**

```
execute set system session filter src <ip_range>
```

**To specify virtual domain**

```
execute set system session filter vd <vdom_index>
```

Variable	Description
<duration_range>	The start and end times, separated by a space.
<expire_range>	The start and end times, separated by a space.
<ip_range>	The start and end IP addresses, separated by a space.
<policy_range>	The start and end policy numbers, separated by a space.

Variable	Description
<port_range>	The start and end port numbers, separated by a space.
<protocol_range>	The start and end protocol numbers, separated by a space.
<vdom_index>	The VDOM index number. -1 means all VDOMs.

## set-next-reboot

Use this command to start the FortiGate unit with primary or secondary firmware after the next reboot. Available on models that can store two firmware images. By default, the FortiGate unit loads the firmware from the primary partition.

VDOM administrators do not have permission to run this command. It must be executed by a super administrator.

### Syntax

```
execute set-next-reboot {primary | secondary}
```

## sfp-mode-sgmii

Change the SFP mode for an NP2 card to SGMII. By default when an AMC card is inserted the SFP mode is set to SERDES mode by default.

If a configured NP2 card is removed and re-inserted, the SFP mode goes back to the default.

In these situations, the `sfpmode-sgmii` command will change the SFP mode from SERDES to SGMII for the interface specified.

### Syntax

```
execute sfpmode-sgmii <interface>
```

<interface> is the NP2 interface where you are changing the SFP mode.

## shutdown

Shut down the FortiGate unit now. You will be prompted to confirm this command.

---

Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

---

### Syntax

```
execute shutdown [comment <comment_string>]
```

`comment` is optional but you can use it to add a message that will appear in the event log message that records the shutdown. The `comment` message of the does not appear on the Alert Message console. If the message is more than one word it must be enclosed in quotes.

### Example

This example shows the reboot command with a message included.

```
execute shutdown comment "emergency facility shutdown"
```

An event log message similar to the following is recorded:

```
2009-09-08 11:12:31 critical admin 41986 ssh(172.20.120.11) shutdown User admin shutdown
the device from ssh(172.20.120.11). The reason is 'emergency facility shutdown'
```

## ssh

Use this command to establish an ssh session with another system.

### Syntax

```
execute ssh <destination> [<port>]
```

<destination> - the destination in the form `user@ip` or `user@host`.

[<port>] - optional TCP port number

### Example

```
execute ssh admin@172.20.120.122
```

To end an ssh session, type `exit`:

```
FGT-6028030112 # exit
Connection to 172.20.120.122 closed.
FGT-8002805000 #
```

## sync-session

Use this command to force a session synchronization.

### Syntax

```
execute sync-session
```

## system custom-language import

Use this command to import a custom language file from a TFTP server.

The web-based manager provides a downloadable template file. Go to *System > Config > Advanced*.

### Syntax

```
execute system custom-language import <lang_name> <file_name> <tftp_server_ip>
```

<lang\_name> - language name

<file\_name> - the language file name

<tftp\_server\_ip> the TFTP server IP address

## system fortisandbox test-connectivity

Use this command to query FortiSandbox connection status.

### Syntax

```
execute system fortisandbox test-connectivity
```

## tac report

Use this command to create a debug report to send to Fortinet Support. Normally you would only use this command if requested to by Fortinet Support.

### Syntax

```
execute tac report
```

## telnet

Use telnet client. You can use this tool to test network connectivity.

### Syntax

```
execute telnet <telnet_ipv4>  
<telnet_ipv4> is the address to connect with.
```

Type `exit` to close the telnet session.

## time

Get or set the system time.

### Syntax

```
execute time [<time_str>  
time_str has the form hh:mm:ss, where  
hh is the hour and can be 00 to 23  
mm is the minutes and can be 00 to 59  
ss is the seconds and can be 00 to 59
```

If you do not specify a time, the command returns the current system time.

You are allowed to shorten numbers to only one digit when setting the time. For example both 01:01:01 and 1:1:1 are allowed.

### Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

## traceroute

Test the connection between the FortiGate unit and another network device, and display information about the network hops between the device and the FortiGate unit.

### Syntax

```
execute traceroute {<ip_address> | <host-name>}
```

### Example

This example shows how to test the connection with <http://docs.forticare.com>. In this example the traceroute command times out after the first hop indicating a possible problem.

```
#execute traceoute docs.forticare.com
traceroute to docs.forticare.com (65.39.139.196), 30 hops max, 38 byte packets
1 172.20.120.2 (172.20.120.2) 0.324 ms 0.427 ms 0.360 ms
2 * * *
```

If your FortiGate unit is not connected to a working DNS server, you will not be able to connect to remote host-named locations with traceroute.

## tracert6

Test the connection between the FortiGate unit and another network device using IPv6 protocol, and display information about the network hops between the device and the FortiGate unit.

### Syntax

```
tracert6 [-Fdn] [-f first_ttl] [-i interface] [-m max_ttl]
[-s src_addr] [-q nprobes] [-w waittime] [-z sendwait]
host [paddatalen]
```

Variable	Description
-F	Set Don't Fragment bit.
-d	Enable debugging.
-n	Do not resolve numeric address to domain name.

Variable	Description
-f <first_ttl>	Set the initial time-to-live used in the first outgoing probe packet.
-i <interface>	Select interface to use for tracer.
-m <max_ttl>	Set the max time-to-live (max number of hops) used in outgoing probe packets.
-s <src_addr>	Set the source IP address to use in outgoing probe packets.
-q <nprobes>	Set the number probes per hop.
-w <waittime>	Set the time in seconds to wait for response to a probe. Default is 5.
-z <sendwait>	Set the time in milliseconds to pause between probes.
host	Enter the IP address or FQDN to probe.
<paddatalen>	Set the packet size to use when probing.

## update-av

Use this command to manually initiate the virus definitions and engines update. To update both virus and attack definitions, use the `execute update-now` command.

### Syntax

```
execute update-av
```

## update-geo-ip

Use this command to obtain an update to the IP geography database from FortiGuard.

### Syntax

```
execute update-geo-ip
```

## update-ips

Use this command to manually initiate the Intrusion Prevention System (IPS) attack definitions and engine update. To update both virus and attack definitions, use the `execute update-now` command.

### Syntax

```
execute update-ips
```

## update-list

Use this command to download an updated FortiGuard server list.

### Syntax

```
execute update-list
```

## update-now

Use this command to manually initiate both virus and attack definitions and engine updates. To initiate only virus or attack definitions, use the `execute update-av` or `execute update-ids` command respectively.

### Syntax

```
execute update-now
```

## update-src-vis

Use this command to trigger an FDS update of the source visibility signature package.

### Syntax

```
execute update-src-vis
```

## upd-vd-license

Use this command to enter a Virtual Domain (VDOM) license key.

If you have a FortiGate- unit that supports VDOM licenses, you can purchase a license key from Fortinet to increase the maximum number of VDOMs to 25, 50, 100 or 500. By default, FortiGate units support a maximum of 10 VDOMs.

Available on FortiGate models that can be licensed for more than 10 VDOMs.

### Syntax

```
execute upd-vd-license <license_key>
```

Variable	Description
<license_key>	The license key is a 32-character string supplied by Fortinet. Fortinet requires your unit serial number to generate the license key.



## upload

Use this command to upload system configurations and firmware images to the flash disk from FTP, TFTP, or USB sources.

### Syntax

#### To upload configuration files:

```
execute upload config ftp <filename_str> <comment> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute upload config tftp <filename_str> <comment> <server_ipv4>
execute upload config usb <filename_str> <comment>
```

#### To upload firmware image files:

```
execute upload image ftp <filename_str> <comment> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute upload image tftp <filename_str> <comment> <server_ipv4>
execute upload image usb <filename_str> <comment>
```

#### To upload report image files:

```
execute upload report-img ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute upload report-img tftp <filename_str> <server_ipv4>
```

Variable	Description
<comment>	Comment string.
<filename_str>	Filename to upload.
<server_fqdn[:port_int]>	Server fully qualified domain name and optional port.
<server_ipv4[:port_int]>	Server IP address and optional port number.
<username_str>	Username required on server.
<password_str>	Password required on server.
<backup_password_str>	Password for backup file.

## usb-device

Use these commands to manage FortiExplorer IOS devices.

## Syntax

### List connected FortiExplorer IOS devices

```
execute usb-device list
```

### Disconnect FortiExplorer IOS devices

```
execute usb-device disconnect
```

## usb-disk

Use these commands to manage your USB disks.

## Syntax

```
execute usb-disk delete <filename>
execute usb-disk format
execute usb-disk list
execute usb-disk rename <old_name> <new_name>
```

Variable	Description
delete <filename>	Delete the named file from the USB disk.
format	Format the USB disk.
list	List the files on the USB disk.
rename <old_name> <new_name>	Rename a file on the USB disk.

## vpn certificate ca

Use this command to import a CA certificate from a TFTP or SCEP server to the FortiGate unit, or to export a CA certificate from the FortiGate unit to a TFTP server.

Before using this command you must obtain a CA certificate issued by a CA.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

---

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

---

## Syntax

```
execute vpn certificate ca export tftp <certificate-name_str> <file-name_str> <tftp_ip>
execute vpn certificate ca import auto <ca_server_url> <ca_identifier_str>
execute vpn certificate ca import tftp <file-name_str> <tftp_ip>
```

Variable	Description
import	Import the CA certificate from a TFTP server to the FortiGate unit.
export	Export or copy the CA certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the CA certificate.
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.
auto	Retrieve a CA certificate from a SCEP server.
tftp	Import the CA certificate to the FortiGate unit from a file on a TFTP server (local administrator PC).
<ca_server_url>	Enter the URL of the CA certificate server.
<ca_identifier_str>	CA identifier on CA certificate server (optional).

## Examples

Use the following command to import the CA certificate named `trust_ca` to the FortiGate unit from a TFTP server with the address `192.168.21.54`.

```
execute vpn certificate ca import trust_ca 192.168.21.54
```

## vpn certificate crl

Use this command to get a CRL via LDAP, HTTP, or SCEP protocol, depending on the auto-update configuration.

In order to use the command `execute vpn certificate crl`, the authentication servers must already be configured.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

---

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

---

## Syntax

```
execute vpn certificate crl import auto <crl-name>
```

Variable	Description
import	Import the CRL from the configured LDAP, HTTP, or SCEP authentication server to the FortiGate unit.
<crl-name>	Enter the name of the CRL.
auto	Trigger an auto-update of the CRL from the configured LDAP, HTTP, or SCEP authentication server.

## vpn certificate local export

Use this command to export a local certificate from the FortiGate unit to a TFTP server.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

---

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

---

## Syntax

```
execute vpn certificate local export tftp <certificate-name_str> <file-name_str> <tftp_ip>
```

Variable	Description
export	Export or copy the local certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the local certificate.  To view a list of the local certificates, you can enter:  execute vpn certificate local export tftp ?
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.

## Example

Use the following command to export the local certificate request generated in the above example from the FortiGate unit to a TFTP server. The example uses the file name `testcert` for the downloaded file and the

TFTP server address 192.168.21.54.

```
execute vpn certificate local export branch_cert testcert 192.168.21.54
```

## vpn certificate local generate

Use this command to generate a local certificate.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

When you generate a certificate request, you create a private and public key pair for the local FortiGate unit. The public key accompanies the certificate request. The private key remains confidential.

When you receive the signed certificate from the CA, use the `vpn certificate local` command to install it on the FortiGate unit.

---

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

---

### Syntax

#### To generate the default CA certificate used by SSL Inspection

```
execute vpn certificate local generate default-ssl-ca
```

#### To generate the default server key used by SSL Inspection

```
execute vpn certificate local generate default-ssl-serv-key
```

#### To generate an elliptical curve certificate request

```
execute vpn certificate local generate ec <certificate-name_str> <elliptic-curve-name>
<subject_str> [<optional_information>]
```

#### To generate an RSA certificate request

```
execute vpn certificate local generate rsa <certificate-name_str> <key-length>
<subject_str> [<optional_information>]
```

Variable	Description
<certificate-name_str>	Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

Variable	Description
<elliptic-curve-name>	Enter the elliptic curve name: <code>secp256r1</code> , <code>secp384r1</code> , or <code>secp521r1</code> .
<key-length>	Enter 1024, 1536 or 2048 for the size in bits of the encryption key.
<subject_str>	<p>Enter the FortiGate unit host IP address, its fully qualified domain name, or an email address to identify the FortiGate unit being certified.</p> <p>An IP address or domain name is preferred. If this is impossible (such as with a dialup client), use an e-mail address.</p> <p>If you specify a host IP or domain name, use the IP address or domain name associated with the interface on which IKE negotiations will take place (usually the external interface of the local FortiGate unit). If the IP address in the certificate does not match the IP address of this interface (or if the domain name in the certificate does not match a DNS query of the FortiGate unit's IP), then some implementations of IKE may reject the connection. Enforcement of this rule varies for different IPSec products.</p>
[<optional_information>]	<p>Enter <code>optional_information</code> as required to further identify the certificate. See <a href="#">Optional information variables on page 390</a> for the list of optional information variables. You must enter the optional variables in order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list. For example, to enter the <code>organization_name_str</code>, you must first enter the <code>country_code_str</code>, <code>state_name_str</code>, and <code>city_name_str</code>. While entering optional variables, you can type <code>?</code> for help on the next required variable.</p>

### Optional information variables

Variable	Description
<country_code_str>	Enter the two-character country code. Enter <code>execute vpn certificates local generate &lt;name_str&gt; country</code> followed by a <code>?</code> for a list of country codes. The country code is case sensitive. Enter <code>null</code> if you do not want to specify a country.
<state_name_str>	Enter the name of the state or province where the FortiGate unit is located.

Variable	Description
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiGate unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiGate unit.
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit.
<email_address_str>	Enter a contact e-mail address for the FortiGate unit.
<ca_server_url>	Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request.
<challenge_password>	Enter the challenge password for the SCEP certificate server.

### Example

Use the following command to generate a local certificate request with the name `branch_cert`, the domain name `www.example.com` and a key size of 1536.

```
execute vpn certificate local generate branch_cert 1536 www.example.com
```

## vpn certificate local import

Use this command to import a local certificate to the FortiGate unit from a TFTP server.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

---

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

---

### Syntax

```
execute vpn certificate local import tftp <file-name_str> <tftp_ip>
```

Variable	Description
<certificate-name_str>	Enter the name of the local certificate.

Variable	Description
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.

### Example

Use the following command to import the signed local certificate named `branch_cert` to the FortiGate unit from a TFTP server with the address 192.168.21.54.

```
execute vpn certificate local import branch_cert 192.168.21.54
```

## vpn certificate remote

Use this command to import a remote certificate from a TFTP server, or export a remote certificate from the FortiGate unit to a TFTP server. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

### Syntax

```
execute vpn certificate remote import tftp <file-name_str> <tftp_ip>
execute vpn certificate remote export tftp <certificate-name_str> <file-name_str>
<tftp_ip>
```

Field/variable	Description
import	Import the remote certificate from the TFTP server to the FortiGate unit.
export	Export or copy the remote certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the public certificate.
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.
tftp	Import/export the remote certificate via a TFTP server.

## vpn ipsec tunnel down

Use this command to shut down an IPsec VPN tunnel.

### Syntax

```
execute vpn ipsec tunnel down <phase2> [<phase1> <phase2_serial>]
```

where:



<phase2> is the phase 2 name

<phase1> is the phase 1 name

<phase2\_serial> is the phase 2 serial number

<phase1> is required on a dial-up tunnel.

## vpn ipsec tunnel up

Use this command to activate an IPsec VPN tunnel.

### Syntax

```
execute vpn ipsec tunnel up <phase2> [<phase1> <phase2_serial>]
```

where:

<phase2> is the phase 2 name

<phase1> is the phase 1 name

<phase2\_serial> is the phase 2 serial number

This command cannot activate a dial-up tunnel.

## vpn sslvpn del-all

Use this command to delete all SSL VPN connections in this VDOM.

### Syntax

```
execute vpn sslvpn del-all
```

## vpn sslvpn del-tunnel

Use this command to delete an SSL tunnel connection.

### Syntax

```
execute vpn sslvpn del-tunnel <tunnel_index>
```

<tunnel\_index> identifies which tunnel to delete if there is more than one active tunnel.

## vpn sslvpn del-web

Use this command to delete an active SSL VPN web connection.

### Syntax

```
execute vpn sslvpn del-web <web_index>
```

<web\_index> identifies which web connection to delete if there is more than one active connection.

## vpn sslvpn list

Use this command to list current SSL VPN tunnel connections.

### Syntax

```
execute vpn sslvpn list {web | tunnel}
```

## webfilter quota-reset

Use this command to reset user quota.

### Syntax

```
execute webfilter quota-reset <wf-profile> <user_ip4addr>
execute webfilter quota-reset <wf-profile> <user_name>
```

## wireless-controller delete-wtp-image

Use this command to delete all firmware images for WLAN Termination Points (WTPs), also known as physical access points.

### Syntax

```
execute wireless-controller delete-wtp-image
```

## wireless-controller list-wtp-image

Use this command to list all firmware images for WLAN Termination Points (WTPs), also known as WiFi physical access points.

### Syntax

```
execute wireless-controller list-wtp-image
```

### Example output

```
WTP Images on AC:
ImageName ImageSize(B) ImageInfo ImageMTime
FAP22A-IMG.wtp 3711132 FAP22A-v4.0-build212 Mon Jun 6 12:26:41 2011
```

## wireless-controller reset-wtp

Use this command to reset a physical access point (WTP).

If the FortiGate unit has a more recent version of the FortiAP firmware, the FortiAP unit will download and install it. Use the command [execute wireless-controller upload-wtp-image](#) to upload FortiAP firmware to the FortiGate unit.

### Syntax

```
execute wireless-controller reset-wtp {<serialNumber_str> | all}
```

where <serialNumber\_str> is the FortiWiFi unit serial number.

Use the `all` option to reset all APs.

## wireless-controller restart-acd

Use this command to restart the wireless-controller daemon.

### Syntax

```
execute wireless-controller restart-acd
```

## wireless-controller restart-wtpd

Use this command to restart the wireless access point daemon.

### Syntax

```
execute wireless-controller restart-wtpd
```

## wireless-controller upload-wtp-image

Use this command to upload a FortiWiFi firmware image to the FortiGate unit. Wireless APs controlled by this wireless controller can download the image as needed. Use the [execute wireless-controller reset-wtp](#) command to trigger FortiAP units to update their firmware.

### Syntax

FTP:

```
execute wireless-controller upload-wtp-image ftp <filename_str> <server_ipv4[:port_
int]> [<username_str> <password_str>]
```

TFTP:

```
execute wireless-controller upload-wtp-image tftp <filename_str> <server_ipv4>
```

# get

The get commands retrieve information about the operation and performance of your FortiGate unit.

## application internet-service status

Use this command to display Internet service information.

### Syntax

```
get application internet-service status [<app-id>]
```

All application IDs are listed if <app-id> is not specified.

### Example output

```
FG-5KD3914800284 # get application internet-service status 1245324
id: 1245324 app-name: "Fortinet-FortiGuard"
```

## application internet-service-summary

Use this command to display information about the Internet service database.

### Syntax

```
get application internet-service-summary
```

### Example output

```
FG-5KD3914800284 # get application internet-service-summary
Version: 00002.00679
Timestamp: 201512161002
Number of Entries: 1267
```

## certificate

Display detailed information about local and CA certificates installed on the FortiGate. This is a global level command. At the VDOM level, use `get vpn certificate`.

### Syntax

```
get certificate {local | ca} details [certificate_name]
```

## extender modem-status

Use this command to display detailed FortiExtender modem status information.

### Syntax

```
get extender modem-status <serno>
```

where <serno> is the FortiExtender serial number.

### Example output

```
physical_port: Internal
manufacture: Sierra Wireless, Incorporated
product: AirCard 313U
model: AirCard 313U
revision: SWI9200X_03.05.10.02AP R4684 CARMD-EN-10527 2012/02/25 11:58:38
imsi: 310410707582825
pin_status: READY
service: N/A
signal_strength: 73
RSSI: -68 dBm
connection_status: connected
Profile 1: broadband
Profile 2: broadband
Profile 13: wap.cingular
Profile 15: broadband
NAI: w.tp
Profile: 0 Disabled
home_addr: 127.219.10.128
primary_ha: 127.218.246.40
secondary_ha: 119.75.69.176
aaa_spi: 0
ha_spi: 4
esn_imei: 012615000227604
activation_status: Activated
roaming_status: N/A
usim_status: N/A
oma_dm_version: N/A
plmn: N/A
band: B17
signal_rsrq: N/A
signal_rsrp: N/A
lte_sinr: N/A
lte_rssi: N/A
lte_rs_throughput: N/A
lte_ts_throughput: N/A
lte_physical_cellid: N/A
modem_type:
drc_cdma_evdo: N/A
current_snr: N/A
wireless_operator:
operating_mode: N/A
wireless_signal: 73
usb_wan_mac: 16:78:f7:db:01:07
```

## extender sys-info

Use this command to display detailed FortiExtender system information.

### Syntax

```
get extender sys-info
```

## firewall dnstranslation

Use this command to display the firewall DNS translation table.

### Syntax

```
get firewall dnstranslation
```

## firewall iprope appctrl

Use this command to list all application control signatures added to an application control list and display a summary of the application control configuration.

### Syntax

```
get firewall iprope appctrl {list | status}
```

### Example output

In this example, the FortiGate unit includes one application control list that blocks the FTP application.

```
get firewall iprope appctrl list
app-list=app_list_1/2000 other-action=Pass
app-id=15896 list-id=2000 action=Block
```

```
get firewall iprope appctrl status
appctrl table 3 list 1 app 1 shaper 0
```

## firewall iprope list

Use this command to list all of the FortiGate unit iprope firewall policies. Optionally include a group number in hexadecimal format to display a single policy. Policies are listed in FortiOS format.

### Syntax

```
get firewall iprope list [<group_number_hex>]
```

### Example output

```
get firewall iprope list 0010000c

policy flag (80000000): pol_stats
flag2 (20): ep_block shapers: / per_ip=
imflag: sockport: 1011 action: redirect index: 0
schedule() group=0010000c av=00000000 au=00000000 host=0 split=00000000
chk_client_info=0x0 app_list=0 misc=0 grp_info=0 seq=0 hash=0
npu_sensor_id=0
tunnel=
zone(1): 0 ->zone(1): 0
source(0):
dest(0):
source wildcard(0):
destination wildcard(0):
service(1):
[6:0x8:1011/(0,65535)->(80,80)]
nat(0):
mms: 0 0
```

## firewall proute, proute6

Use these commands to list policy routes.

### Syntax

For IPv4 policy routes:

```
get firewall proute
```

For IPv6 policy routes:

```
get firewall proute6
```

### Example output

```
get firewall proute
list route policy info(vf=root):
iff=5 src=1.1.1.0/255.255.255.0 tos=0x00 tos_mask=0x00 dst=0.0.0.0/0.0.0.0 protocol=80
port=1:65535
oif=3 gwy=1.2.3.4
```

## firewall service custom

Use this command to view the list of custom services. If you do not specify a <service\_name> the command lists all of the pre-defined services.

### Syntax

```
get firewall service custom
```

This lists the services.

**To view details about all services**

```
config firewall service custom
show full-configuration
```

**To view details about a specific service**

This example lists the configuration for the ALL\_TCP service:

```
config firewall service custom
edit ALL_TCP
show full-configuration
```

**Example output**

This is a partial output.

```
get firewall service custom
== [ ALL ]
name: ALL
== [ ALL_TCP ]
name: ALL_TCP
== [ ALL_UDP ]
name: ALL_UDP
== [ ALL_ICMP ]
name: ALL_ICMP
== [ ALL_ICMP6 ]
name: ALL_ICMP6
== [ GRE ]
name: GRE
== [ AH ]
name: AH
== [ ESP ]
name: ESP
== [ AOL ]
name: AOL
== [ BGP ]
name: BGP
== [ DHCP ]
name: DHCP
== [ DNS ]
name: DNS
== [ FINGER ]
name: FINGER
```

## firewall shaper

Use these command to retrieve information about traffic shapers.

**Syntax****To get information about per-ip traffic shapers**

```
get firewall shaper per-ip
```



## To get information about shared traffic shapers

```
get firewall shaper traffic-shaper
```

## grep

In many cases the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large `get` or `show` command output you can use the `grep` command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX `grep`, used for searching text output based on regular expressions.

Information about how to use `grep` and regular expressions is available from the Internet. For example, see <http://www.opengroup.org/onlinepubs/009695399/utilities/grep.html>.

### Syntax

```
{get | show | diagnose} | grep <regular_expression>
```

### Example output

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr 00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
19:tcp 1110 10.31.101.10:1862 172.20.120.122:30670 69.111.193.57:1469 -
27:tcp 3599 10.31.101.10:2061 - 10.31.101.100:22 -
38:tcp 3594 10.31.101.10:4780 172.20.120.122:49700 172.20.120.100:445 -
43:tcp 3582 10.31.101.10:4398 172.20.120.122:49574 24.200.188.171:48726 -
```

Use the following command to display all lines in HTTP replacement message commands that contain URL (upper or lower case):

```
show system replacemsg http | grep -i url
set buffer "<HTML><BODY>The page you requested has been blocked because it contains a
  banned word. URL = %%PROTOCOL%%URL%%</BODY></HTML>"
config system replacemsg http "url-block"
set buffer "<HTML><BODY>The URL you requested has been blocked. URL =
  %%URL%%</BODY></HTML>"
config system replacemsg http "urlfilter-err"
.
.
.
```

## gui console status

Display information about the CLI console.

### Syntax

```
get gui console status
```

## Example

The output looks like this:

```
Preferences:
    User: admin
        Colour scheme (RGB): text=FFFFFF, background=000000
        Font: style=monospace, size=10pt
        History buffer=50 lines, external input=disabled
```

## hardware cpu

Use this command to display detailed information about all of the CPUs in your FortiGate unit.

### Syntax

```
get hardware cpu
```

### Example output

```
get hardware npu legacy list
No npu ports are found
```

```
620_ha_1 # get hardware cpu
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 15
model name : Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
stepping : 13
cpu MHz : 1795.545
cache size : 64 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 10
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
        dts acpi mmx fxsr sse sse2 ss ht tm pbe lm pni monitor ds_cpl tm2 est
bogomips : 3578.26

processor : 1
vendor_id : GenuineIntel
cpu family : 6
model : 15
model name : Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
stepping : 13
cpu MHz : 1795.545
cache size : 64 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
```

```
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 10
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
      dts acpi mmx fxsr sse sse2 ss ht tm pbe lm pni monitor ds_cpl tm2 est
bogomips : 3578.26
```

## hardware memory

Use this command to display information about FortiGate unit memory use including the total, used, and free memory.

### Syntax

```
get hardware memory
```

### Example output

```
get hardware memory
total: used: free: shared: buffers: cached: shm:
Mem: 3703943168 348913664 3355029504 0 192512 139943936 137314304
Swap: 0 0 0
MemTotal: 3617132 kB
MemFree: 3276396 kB
MemShared: 0 kB
Buffers: 188 kB
Cached: 136664 kB
SwapCached: 0 kB
Active: 22172 kB
Inactive: 114740 kB
HighTotal: 1703936 kB
HighFree: 1443712 kB
LowTotal: 1913196 kB
LowFree: 1832684 kB
SwapTotal: 0 kB
SwapFree: 0 kB
```

## hardware nic

Use this command to display hardware and status information about each FortiGate interface. The hardware information includes details such as the driver name and version and chip revision. Status information includes transmitted and received packets, and different types of errors.

### Syntax

```
get hardware nic <interface_name>
```

Variable	Description
<interface_name>	A FortiGate interface name such as port1, wan1, internal, etc.

### Example output

```

get hardware nic port9
Chip_Model FA2/ISCP1B-v3/256MB
FPGA_REV_TAG 06101916
Driver Name iscpla/b-DE
Driver Version 0.1
Driver Copyright Fortinet Inc.

Link down
Speed N/A
Duplex N/A
State up

Rx_Packets 0
Tx_Packets 0
Rx_Bytes 0
Tx_Bytes 0

Current_HWaddr 00:09:0f:77:09:68
Permanent_HWaddr 00:09:0f:77:09:68

Frame_Received 0
Bad Frame Received 0
Tx Frame 0
Tx Frame Drop 0
Receive IP Error 0
FIFO Error 0

Small PktBuf Left 125
Normal PktBuf Left 1021
Jumbo PktBuf Left 253
NAT Anomaly 0

```

## hardware npu

Use this command to display information about the network processor unit (NPU) hardware installed in a FortiGate unit. The NPUs can be built-in or on an installed AMC module.

### Syntax

```

get hardware npu legacy {list | session <device_name_str> | setting <device_name_str>}
get hardware npu np1 {list | status}
get hardware npu np2 {list | performance <device_id_int> | status <device_id_int>}
get hardware npu np4 {list | status <device_id_int>}
get hardware npu np6 {dce | ipsec-stats | port-list | session-stats <device_id_int> |
    sse-stats <device_id_int> | synproxy-stats}
get hardware npu sp {list | status}

```

## Example output

```

get hardware npu np1 list
ID Interface
0 port9 port10

get hardware npu np1 status
ISCP1A 10ee:0702
RX SW Done 0 MTP 0x00000000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Total Number of Interfaces: 2
Number of Interface In-Use: 2
Interface[0] Tx done: 0
desc_size = 0x00004000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
Interface[1] Tx done: 0
desc_size = 0x00004000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
NAT Information:
head = 0x00000001 tail = 00000001
ISCP1A Performance [Top]:
Nr_int : 0x00000000 INTwoInd : 0x00000000 RXwoDone : 0x00000000
PKTwoEnd : 0x00000000 PKTCSErr : 0x00000000
PKTidErr : 0x00000000 PHY0Int : 0x00000000 PHY1INT : 0x00000000
CSUMOFF : 0x00000000 BADCSUM : 0x00000000 MSGINT : 0x00000000
IPSEC : 0x00000000 IPSVLAN : 0x00000000 SESMISS : 0x00000000
TOTUP : 0x00000000 RSVD MEMU : 0x00000010
MSG Performance:
QLEN: 0x00001000(QW) HEAD: 0x00000000
Performance:
TOTMSG: 0x00000000 BADMSG: 0x00000000 TOUTMSG: 0x00000000 QUERY: 0x00000000
NULLTK: 0x00000000
NAT Performance: BYPASS (Enable) BLOCK (Disable)
IRQ : 00000001 QFTL : 00000000 DELF : 00000000 FFTL : 00000000
OVTH : 00000001 QRYF : 00000000 INSF : 00000000 INVC : 00000000
ALLO : 00000000 FREE : 00000000 ALLOF : 00000000 BPENTR: 00000000 BKENTR: 00000000
PBPENTR: 00000000 PBKENTR: 00000000 NOOP : 00000000 THROT : 00000000(0x002625a0)
SWITOT : 00000000 SWDTOT : 00000000 ITDB : 00000000 OTDB : 00000000
SPISES : 00000000 FLUSH : 00000000
APS (Disabled) information:
MODE: BOTH UDPTH 255 ICMPTH 255 APSFLAGS: 0x00000000
IPSEC Offload Status: 0x58077dcb

get hardware npu np2 list
ID PORTS
-- -----
0 amc-sw1/1
0 amc-sw1/2
0 amc-sw1/3
0 amc-sw1/4
ID PORTS

```

```

-- -----
1 amc-dw2/1
ID PORTS
-- -----
2 amc-dw2/2

get hardware npu np2 status 0
NP2 Status

ISCP2 f7750000 (Neighbor 00000000) 1a29:0703 256MB Base f8aad000 DBG 0x00000000
RX SW Done 0 MTP 0x0
desc_alloc = f7216000
desc_size = 0x2000 count = 0x100
nxt_to_u = 0x0 nxt_to_f = 0x0
Total Interfaces: 4 Total Ports: 4
Number of Interface In-Use: 4
Interface f7750100 netdev 81b1e000 0 Name amc-sw1-1
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750694, 00000000, 00000000, 00000000
Port f7750694 Id 0 Status Down ictr 4
desc = 8128c000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f7750100
Interface f7750264 netdev 81b2cc00 1 Name amc-sw1-2
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750748, 00000000, 00000000, 00000000
Port f7750748 Id 1 Status Down ictr 0
desc = 81287000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f7750264
Interface f77503c8 netdev 81b2c800 2 Name amc-sw1-3
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77507fc, 00000000, 00000000, 00000000
Port f77507fc Id 2 Status Down ictr 0
desc = 81286000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f77503c8
Interface f775052c netdev 81b2c400 3 Name amc-sw1-4
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77508b0, 00000000, 00000000, 00000000
Port f77508b0 Id 3 Status Down ictr 0
desc = 81281000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f775052c
NAT Information:
cmdq_qw = 0x2000 cmdq = 82160000
head = 0x1 tail = 0x1
APS (Enabled) information:
Session Install when TMM TSE OOE: Disable
Session Install when TMM TAE OOE: Disable
IPS anomaly check policy: Follow config
MSG Base = 82150000 QL = 0x1000 H = 0x0

```

## hardware status

Report information about the FortiGate unit hardware including FortiASIC version, CPU type, amount of memory, flash drive size, hard disk size (if present), USB flash size (if present), network card chipset, and WiFi chipset (FortiWiFi models). This information can be useful for troubleshooting, providing information about your FortiGate unit to Fortinet Support, or confirming the features that your FortiGate model supports.

### Syntax

```
get hardware status
```

### Example output

```
Model name: Fortigate-620B
ASIC version: CP6
ASIC SRAM: 64M
CPU: Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
RAM: 2020 MB
Compact Flash: 493 MB /dev/sda
Hard disk: 76618 MB /dev/sdb
USB Flash: not available
Network Card chipset: Broadcom 570x Tigon3 Ethernet Adapter (rev.0x5784100)
```

## ips decoder status

Displays all the port settings of all the IPS decoders.

### Syntax

```
get ips decoder status
```

### Example output

```
# get ips decoder status
decoder-name: "back_orifice"

decoder-name: "dns_decoder"
port_list: 53

decoder-name: "ftp_decoder"
port_list: 21

decoder-name: "http_decoder"

decoder-name: "im_decoder"

decoder-name: "imap_decoder"
port_list: 143
```

Ports are shown only for decoders with configurable port settings.

## ips rule status

Displays current configuration information about IPS rules.

### Syntax

```
get ips rule status
```

### Example output

```
# get ips rule status
rule-name: "IP.Land"
rule-id: 12588
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 3.high
service: All
location: server, client
os: All
application: All

rule-name: "IP.Loose.Src.Record.Route.Option"
rule-id: 12805
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 2.medium
service: All
location: server, client
os: All
application: All
```

## ips session

Displays current IPS session status.

### Syntax

```
get ips session
```

### Example output

```
get ips session

SYSTEM:
memory capacity 279969792
memory used 5861008
```



```
recent pps\bps 0\0K
session in-use 0
TCP: in-use\active\total 0\0\0
UDP: in-use\active\total 0\0\0
ICMP: in-use\active\total 0\0\0
```

## ips view-map

Use this command to view the policies examined by IPS. This is mainly used for debugging. If there is no ips view map, it means IPS is not used or enabled.

### Syntax

```
get ips view-map <id>
```

### Example output

```
id : 1
id-policy-id : 0
policy-id : 2
vdom-id : 0
which : firewall
```

Variable	Description
id	IPS policy ID
id-policy-id	Identity-based policy ID (0 means none)
policy-id	Policy ID
vdom-id	VDOM, identified by ID number
which	Type of policy id: firewall, firewall6, sniffer, sniffer6, interface, interface6

## ipsec tunnel

List the current IPsec VPN tunnels and their status.

### Syntax

**To view details of all IPsec tunnels:**

```
get ipsec tunnel details
```

**To list IPsec tunnels by name:**

```
get ipsec tunnel name
```

**To view a summary of IPsec tunnel information:**

```
get ipsec tunnel summary
```

## mgmt-data status

Use this command to display information additional to that provided by `get system status` or `get hardware status`.

### Syntax

```
get mgmt-data status
```

### Sample output

```
FG100D3G12801361 # get mgmt-data status

Model name: FortiGate-100D
CPU: 4
RAM: 1977 MB
is_ssd_available: 0
is_logdisk_mounted: 1
is_support_log_on_boot_device: 1
is_rev_support_wanopt: 1
```

## pbx branch-office

Use this command to list the configured branch offices.

### Syntax

```
get pbx branch-office
```

### Example output

```
== [ Branch 15 ]
name: Branch 15
== [ Branch 12 ]
name: Branch 12
```

## pbx dialplan

Use this command to list the configured dial plans.

### Syntax

```
get pbx dialplan
```

### Example output

```
== [ company-default ]
name: company-default
== [ inbound ]
name: inbound
```

## pbx did

Use this command to list the configured direct inward dial (DID) numbers.

### Syntax

```
get pbx did
```

### Example output

```
== [ Operator ]
name: Operator
== [ Emergency ]
name: Emergency
```

## pbx extension

Use this command to list the configured extensions.

### Syntax

```
get pbx extension
```

### Example output

```
== [ 6555 ]
extension: 6555
== [ 6777 ]
extension: 6777
== [ 6111 ]
extension: 6111
```

## pbx ftgd-voice-pkg

Use this command to display the current FortiGate Voice service package status.

### Syntax

```
get pbx ftgd-voice-pkg status
```

### Example output

```
Status: Activated
Total 1 Packages:
```

```
Package Type: B, Credit Left: 50.00, Credit Used: 0.00,  
Expiration Date: 2011-01-01 12:00:00
```

```
Total 1 Dids:  
12345678901  
Total 1 Efax:  
12345678902  
Total 0 Tollfrees:
```

## pbx global

Use this command to display the current global pbx settings.

### Syntax

```
get pbx global
```

### Example output

```
block-blacklist : enable  
country-area : USA  
country-code : 1  
efax-check-interval : 5  
extension-pattern : 6XXX  
fax-admin-email : faxad@example.com  
ftgd-voice-server : service.fortivoice.com  
local-area-code : 408  
max-voicemail : 60  
outgoing-prefix : 9  
ring-timeout : 20  
rtp-hold-timeout : 0  
rtp-timeout : 60  
voicemail-extension : *97
```

## pbx ringgrp

Use this command to display the currently configured ring groups.

### Syntax

```
get pbx ringgrp
```

### Example output

```
== [ 6001 ]  
name: 6001  
== [ 6002 ]  
name: 6002
```

## pbx sip-trunk

Use this command to display the currently configured SIP trunks.

### Syntax

```
get pbx sip-trunk
```

### Example output

```
== [ __FtgdVoice_1 ]  
name: __FtgdVoice_1
```

## pbx voice-menu

Use this command to display the current voice menu and recorder extension configuration.

### Syntax

```
get pbx voice-menu
```

### Example output

```
comment : general  
password : *  
press-0:  
ring-group : 6001  
type : ring-group  
press-1:  
type : voicemail  
press-2:  
type : directory  
press-3:  
type : none  
press-4:  
type : none  
press-5:  
type : none  
press-6:  
type : none  
press-7:  
type : none  
press-8:  
type : none  
press-9:  
type : none  
recorder-exten : *30
```

## router info bfd neighbor

Use this command to list state information about the neighbors in the bi-directional forwarding table.

### Syntax

```
get router info bfd neighbour
```

## router info bgp

Use this command to display information about the BGP configuration.

### Syntax

```
get router info bgp <keyword>
```

<keyword>	Description
cidr-only	Show all BGP routes having non-natural network masks.
community	Show all BGP routes having their COMMUNITY attribute set.
community-info	Show general information about the configured BGP communities, including the routes in each community and their associated network addresses.
community-list	Show all routes belonging to configured BGP community lists.
dampening	Display information about dampening:
{dampened-paths	Type <code>dampened-paths</code> to show all paths that have been suppressed due to flapping.
flap-statistics	Type <code>flap-statistics</code> to show flap statistics related to BGP routes.
parameters}	Type <code>parameters</code> to show the current dampening settings.
filter-list	Show all routes matching configured AS-path lists.
inconsistent-as	Show all routes associated with inconsistent autonomous systems of origin.
memory	Show the BGP memory table.

<keyword>	Description
neighbors [<address_ipv4>   <address_ipv4> advertised-routes   <address_ipv4> received prefix-filter   <address_ipv4> received-routes   <address_ipv4> routes]	Show information about connections to TCP and BGP neighbors.
network [<address_ ipv4mask>]	Show general information about the configured BGP networks, including their network addresses and associated prefixes.
network-longer- prefixes <address_ ipv4mask>	Show general information about the BGP route that you specify (for example, 12.0.0.0/14) and any specific routes associated with the prefix.
paths	Show general information about BGP AS paths, including their associated network addresses.
prefix-list <name>	Show all routes matching configured prefix list <name>.
quote-regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$) and enable the use of output modifiers (for example, include, exclude, and begin) to search the results.
regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$).
route-map	Show all routes matching configured route maps.
scan	Show information about next-hop route scanning, including the scan interval setting.
summary	Show information about BGP neighbor status.

## Example output

```

get router info bgp memory
Memory type Alloc count Alloc bytes
=====
BGP structure : 2 1408
BGP VR structure : 2 104
BGP global structure : 1 56
BGP peer : 2 3440
BGP as list master : 1 24
Community list handler : 1 32
BGP Damp Reuse List Array : 2 4096
BGP table : 62 248
-----

```

```
Temporary memory : 4223 96095
Hash : 7 140
Hash index : 7 28672
Hash bucket : 11 132
Thread master : 1 564
Thread : 4 144
Link list : 32 636
Link list node : 24 288
Show : 1 396
Show page : 1 4108
Show server : 1 36
Prefix IPv4 : 10 80
Route table : 4 32
Route node : 63 2772
Vector : 2180 26160
Vector index : 2180 18284
Host config : 1 2
Message of The Day : 1 100
IMI Client : 1 708
VTY master : 1 20
VTY if : 11 2640
VTY connected : 5 140
Message handler : 2 120
NSM Client Handler : 1 12428
NSM Client : 1 1268
Host : 1 64
Log information : 2 72
Context : 1 232
```

```
-----
bgp proto specific allocations : 9408 B
bgp generic allocations : 196333 B
bgp total allocations : 205741 B
```

## router info isis

Use this command to display information about the FortiGate ISIS.

### Syntax

```
get router info isis interface
get router info isis neighbor
get router info isis is-neighbor
get router info isis database
get router info isis route
get router info isis topology
```

## router info kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.



## Syntax

```
get router info kernel [<routing_type_int>]
```

## router info multicast

Use this command to display information about a Protocol Independent Multicasting (PIM) configuration. Multicast routing is supported in the root virtual domain only.

## Syntax

```
get router info multicast <keywords>
```

<keywords>	Description
	<p>Show Internet Group Management Protocol (IGMP) membership information according to one of these qualifiers:</p> <p>Type <code>groups</code> [{&lt;interface-name&gt;   &lt;group-address&gt;}] to show IGMP information for the multicast group(s) associated with the specified interface or multicast group address.</p> <p>Type <code>groups-detail</code> [{&lt;interface-name&gt;   &lt;group-address&gt;}] to show detailed IGMP information for the multicast group(s) associated with the specified interface or multicast group address.</p> <p>Type <code>interface</code> [&lt;interface-name&gt;] to show IGMP information for all multicast groups associated with the specified interface.</p> <p>Show information related to dense mode operation according to one of these qualifiers:</p> <p>Type <code>interface</code> to show information about PIM-enabled interfaces.</p> <p>Type <code>interface-detail</code> to show detailed information about PIM-enabled interfaces.</p>
igmp	<p>Type <code>neighbor</code> to show the current status of PIM neighbors.</p> <p>Type <code>neighbor-detail</code> to show detailed information about PIM neighbors.</p> <p>Type <code>next-hop</code> to show information about next-hop PIM routers.</p> <p>Type <code>table</code> [&lt;group-address&gt;] [&lt;source-address&gt;] to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.</p>
pim dense-mode	

<keywords>	Description
	Show information related to sparse mode operation according to one of these qualifiers:
	Type <code>bsr-info</code> to show Boot Strap Router (BSR) information.
	Type <code>interface</code> to show information about PIM-enabled interfaces.
	Type <code>interface-detail</code> to show detailed information about PIM-enabled interfaces.
pim sparse-mode	Type <code>neighbor</code> to show the current status of PIM neighbors.
	Type <code>neighbor-detail</code> to show detailed information about PIM neighbors.
	Type <code>next-hop</code> to show information about next-hop PIM routers.
	Type <code>rp-mapping</code> to show Rendezvous Point (RP) information.
	Type <code>table [&lt;group-address&gt; [&lt;source-address&gt;]</code> to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.
table [<group-address> [<source-address>]	Show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.
table-count [<group-address> [<source-address>]	Show statistics related to the specified multicast group address and/or multicast source address.

## router info ospf

Use this command to display information about the FortiGate OSPF configuration and/or the Link-State Advertisements (LSAs) that the FortiGate unit obtains and generates. An LSA identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination.

### Syntax

```
get router info ospf <keyword>
```

<keyword>	Description
border-routers	Show OSPF routing table entries that have an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) as a destination.

<keyword>	Description
	Show information from the OSPF routing database according to the of these qualifiers.
	Some qualifiers require a <code>target</code> that can be one of the following values:
database <qualifier>	Type <code>adv_router &lt;address_ipv4&gt;</code> to limit the information to LSAs originating from the router at the specified IP address.
	Type <code>self-originate &lt;address_ipv4&gt;</code> to limit the information to LSAs originating from the FortiGate unit.
adv-router <address_ipv4>	Type <code>adv-router &lt;address_ipv4&gt;</code> to show ospf Advertising Router link states for the router at the given IP address.
asbr-summary <target>	Type <code>asbr-summary</code> to show information about ASBR summary LSAs.
brief	Type <code>brief</code> to show the number and type of LSAs associated with each OSPF area.
external <target>	Type <code>external</code> to show information about external LSAs.
max-age	Type <code>max-age</code> to show all LSAs in the MaxAge list.
network <target>	Type <code>network</code> to show information about network LSAs.
nssa-external <target>	Type <code>nssa-external</code> to show information about not-so-stubby external LSAs.
opaque-area <address_ipv4>	Type <code>opaque-area &lt;address_ipv4&gt;</code> to show information about opaque Type 10 (area-local) LSAs (see RFC 2370).
opaque-as <address_ipv4>	Type <code>opaque-as &lt;address_ipv4&gt;</code> to show information about opaque Type 11 LSAs (see RFC 2370), which are flooded throughout the AS.
opaque-link <address_ipv4>	Type <code>opaque-link &lt;address_ipv4&gt;</code> to show information about opaque Type 9 (link-local) LSAs (see RFC 2370).

<keyword>	Description
<code>router</code> <code>&lt;target&gt;</code>	Type <code>router</code> to show information about router LSAs.
<code>self-originate</code>	Type <code>self-originate</code> to show self-originated LSAs.
<code>summary</code> <code>&lt;target&gt;</code>	Type <code>summary</code> to show information about summary LSAs.
<code>interface [&lt;interface_name&gt;]</code>	<p>Show the status of one or all FortiGate interfaces and whether OSPF is enabled on those interfaces.</p> <p>Show general information about OSPF neighbors, excluding down-status neighbors:</p> <p>Type <code>all</code> to show information about all neighbors, including down-status neighbors.</p> <p>Type <code>&lt;neighbor_id&gt;</code> to show detailed information about the specified neighbor only.</p>
<code>neighbor [all   &lt;neighbor_id&gt;   detail   detail all   interface &lt;address_ipv4&gt;]</code>	<p>Type <code>detail</code> to show detailed information about all neighbors, excluding down-status neighbors.</p> <p>Type <code>detail all</code> to show detailed information about all neighbors, including down-status neighbors.</p> <p>Type <code>interface &lt;address_ipv4&gt;</code> to show neighbor information based on the FortiGate interface IP address that was used to establish the neighbor's relationship.</p>
<code>route</code>	Show the OSPF routing table.
<code>status</code>	Show general information about the OSPF routing processes.
<code>virtual-links</code>	Show information about OSPF virtual links.

## router info protocols

Use this command to show the current states of active routing protocols. Inactive protocols are not displayed.

### Syntax

```
get router info protocols
```

```
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
```

```

Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
Routing for Networks:
Routing Information Sources:
Gateway Distance Last Update Bad Packets Bad Routes
Distance: (default is 120)

Routing Protocol is "ospf 0"
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing:
Routing for Networks:
Routing Information Sources: Gateway Distance Last Update
Distance: (default is 110) Address Mask Distance List

Routing Protocol is "bgp 5"
IGP synchronization is disabled
Automatic route summarization is disabled
Default local-preference applied to incoming route is 100
Redistributing:
Neighbor(s):
Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn RouteMapOut Weight
192.168.20.10 unicast

```

## router info rip

Use this command to display information about the RIP configuration.

### Syntax

```
get router info rip <keyword>
```

<keyword>	Description
database	Show the entries in the RIP routing database.
interface	Show the status of the specified FortiGate unit interface
[<interface_name>]	<interface_name> and whether RIP is enabled. If interface is used alone it lists all the FortiGate unit interfaces and whether RIP is enabled on each.

## router info routing-table

Use this command to display the routes in the routing table.

## Syntax

```
get router info routing-table <keyword>
```

<keyword>	Description
all	Show all entries in the routing table.
bgp	Show the BGP routes in the routing table.
connected	Show the connected routes in the routing table.
database	Show the routing information database.
details [<address_ ipv4mask>]	Show detailed information about a route in the routing table, including the next-hop routers, metrics, outgoing interfaces, and protocol-specific information.
ospf	Show the OSPF routes in the routing table.
rip	Show the RIP routes in the routing table.
static	Show the static routes in the routing table.

## router info vrrp

Use this command to display information about the VRRP configuration.

### Syntax

```
get router info vrrp
```

### Example output

```
Interface: port1, primary IP address: 9.1.1.2
VRID: 1
  vrip: 9.1.1.254, priority: 100, state: BACKUP
  adv_interval: 1, preempt: 1, start_time: 3
  vrdest: 0.0.0.0
```

## router info6 bgp

Use this command to display information about the BGP IPv6 configuration.

### Syntax

```
get router info6 bgp <keyword>
```

<keyword>	Description
community	Show all BGP routes having their COMMUNITY attribute set.

<keyword>	Description
community-list	Show all routes belonging to configured BGP community lists.
dampening {dampened-paths   flap-statistics   parameters}	<p>Display information about dampening:</p> <p>Type <code>dampened-paths</code> to show all paths that have been suppressed due to flapping.</p> <p>Type <code>flap-statistics</code> to show flap statistics related to BGP routes.</p> <p>Type <code>parameters</code> to show the current dampening settings.</p>
filter-list	Show all routes matching configured AS-path lists.
inconsistent-as	Show all routes associated with inconsistent autonomous systems of origin.
neighbors [<address_ ipv6mask>	Show information about connections to TCP and BGP neighbors.
network [<address_ ipv6mask>]	Show general information about the configured BGP networks, including their network addresses and associated prefixes.
network-longer-prefixes <address_ ipv6mask>	Show general information about the BGP route that you specify (for example, <code>12.0.0.0/14</code> ) and any specific routes associated with the prefix.
paths	Show general information about BGP AS paths, including their associated network addresses.
prefix-list <name>	Show all routes matching configured prefix list <name>.
quote-regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, <code>^730\$</code> ) and enable the use of output modifiers (for example, <code>include</code> , <code>exclude</code> , and <code>begin</code> ) to search the results.
regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, <code>^730\$</code> ).
route-map	Show all routes matching configured route maps.
summary	Show information about BGP neighbor status.

## router info6 interface

Use this command to display information about IPv6 interfaces.

## Syntax

```
get router info6 interface <interface_name>
```

## Example output

The command returns the status of the interface and the assigned IPv6 address.

```
dmz2 [administratively down/down]  
2001:db8:85a3:8d3:1319:8a2e:370:7348  
fe80::209:fff:fe04:4cfd
```

## router info6 kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

### Syntax

```
get router info6 kernel
```

## router info6 ospf

Use this command to display information about the OSPF IPv6 configuration.

### Syntax

```
get router info6 ospf
```

## router info6 protocols

Use this command to display information about the configuration of all IPv6 dynamic routing protocols.

### Syntax

```
get router info6 protocols
```

## router info6 rip

Use this command to display information about the RIPng configuration.

### Syntax

```
get router info6 rip
```



## router info6 routing-table

Use this command to display the routes in the IPv6 routing table.

### Syntax

```
get router info6 routing-table <item>
```

where <item> is one of the following:

Variable	Description
<ipv6_ip>	Destination IPv6 address or prefix.
bgp	Show BGP routing table entries.
connected	Show connected routing table entries.
database	Show routing information base.
ospf	Show OSPF routing table entries.
rip	Show RIP routing table entries.
static	Show static routing table entries.

## switch-controller poe

Retrieve information about PoE ports.

### Syntax

```
get switch-controller poe <vdom-name> <fortiswitch-id>
```

## system admin list

View a list of all the current administration sessions.

### Syntax

```
get system admin list
```

### Example output

```
# get system admin list
username local  device                remote                started
admin    sshv2  port1:172.20.120.148:22  172.20.120.16:4167  2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443  172.20.120.161:56365  2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443  172.20.120.16:4214  2006-08-09 12:25:29
```

Variable	Description
username	Name of the admin account for this session
local	The protocol this session used to connect to the FortiGate unit.
device	The interface, IP address, and port used by this session to connect to the FortiGate unit.
remote	The IP address and port used by the originating computer to connect to the FortiGate unit.
started	The time the current session started.

## system admin status

View the status of the currently logged in admin and their session.

### Syntax

```
get system admin status
```

### Example

The output looks like this:

```
# get system admin status
username: admin
login local: sshv2
login device: port1:172.20.120.148:22
login remote: 172.20.120.16:4167
login vdom: root
login started: 2006-08-09 12:24:20
current time: 2006-08-09 12:32:12
```

Variable	Description
username	Name of the admin account currently logged in.
login local	The protocol used to start the current session.
login device	The login information from the FortiGate unit including interface, IP address, and port number.
login remote	The computer the user is logging in from including the IP address and port number.
login vdom	The virtual domain the admin is current logged into.
login started	The time the current session started.
current time	The current time of day on the FortiGate unit

## system arp

View the ARP table entries on the FortiGate unit.

This command is not available in multiple VDOM mode.

### Syntax

```
get system arp
```

### Example output

```
# get system arp
Address Age(min) Hardware Addr Interface
172.20.120.16 0 00:0d:87:5c:ab:65 internal
172.20.120.138 0 00:08:9b:09:bb:01 internal
```

## system auto-update

Use this command to display information about the status FortiGuard updates on the FortiGate unit.

### Syntax

```
get system auto-update status
get system auto-update versions
```

### Example output

```
get system auto-update status
FDN availability: available at Thu Apr 1 08:22:58 2010
```

```
Push update: disable
Scheduled update: enable
    Update daily: 8:22
Virus definitions update: enable
IPS definitions update: enable
Server override: disable
Push address override: disable
Web proxy tunneling: disable
```

## system central-management

View information about the Central Management System configuration.

### Syntax

```
get system central-management
```

### Example

The output looks like this:

```
FG600B3908600705 # get system central-management
status : enable
type : fortimanager
auto-backup : disable
schedule-config-restore: enable
schedule-script-restore: enable
allow-push-configuration: enable
allow-pushd-firmware: enable
allow-remote-firmware-upgrade: enable
allow-monitor : enable
fmg : 172.20.120.161
vdom : root
authorized-manager-only: enable
serial-number : "FMG-3K2404400063"
```

## system checksum

View the checksums for global, root, and all configurations. These checksums are used by HA to compare the configurations of each cluster unit.

### Syntax

```
get system checksum status
```

### Example output

```
# get system checksum status
global: 7a 87 3c 14 93 bc 98 92 b0 58 16 f2 eb bf a4 15
root: bb a4 80 07 42 33 c2 ff f1 b5 6e fe e4 bb 45 fb
all: 1c 28 f1 06 fa 2e bc 1f ed bd 6b 21 f9 4b 12 88
```

## system cmdb status

View information about cmdbsvr on the FortiGate unit. FortiManager uses some of this information.

### Syntax

```
get system cmdb status
```

### Example output

```
# get system cmdb status
version: 1
owner id: 18
update index: 6070
config checksum: 12879299049430971535
last request pid: 68
last request type: 29
last request: 78
```

Variable	Description
version	Version of the cmdb software.
owner id	Process ID of the cmdbsvr daemon.
update index	The updated index shows how many changes have been made in cmdb.
config checksum	The config file version used by FortiManager.
last request pid	The last process to access the cmdb.
last request type	Type of the last attempted access of cmdb.
last request	The number of the last attempted access of cmdb.

## system fortianalyzer-connectivity

Display connection and remote disk usage information about a connected FortiAnalyzer unit.

### Syntax

```
get fortianalyzer-connectivity status
```

### Example output

```
# get system fortianalyzer-connectivity status
Status: connected
Disk Usage: 0%
```

## system fortiguard-log-service status

Command returns information about the status of the FortiGuard Log & Analysis Service including license and disk information.

### Syntax

```
get system fortiguard-log-service status
```

### Example output

```
# get system fortiguard-log-service status
FortiGuard Log & Analysis Service
Expire on: 20071231
Total disk quota: 1111 MB
Max daily volume: 111 MB
Current disk quota usage: n/a
```

## system fortiguard-service status

COMMAND REPLACED. Command returns information about the status of the FortiGuard service including the name, version late update, method used for the last update and when the update expires. This information is shown for the AV Engine, virus definitions, attack definitions, and the IPS attack engine.

### Syntax

```
get system fortiguard-service status
```

### Example output

NAME	VERSION	LAST UPDATE	METHOD	EXPIRE
AV Engine	2.002	2006-01-26 19:45:00	manual	2006-06-12 08:00:00
Virus Definitions	6.513	2006-06-02 22:01:00	manual	2006-06-12 08:00:00
Attack Definitions	2.299	2006-06-09 19:19:00	manual	2006-06-12 08:00:00
IPS Attack Engine	1.015	2006-05-09 23:29:00	manual	2006-06-12 08:00:00

## system ha-nonsync-csum

FortiManager uses this command to obtain a system checksum.

### Syntax

```
get system ha-nonsync-csum
```

## system ha status

Use this command to display information about an HA cluster. The command displays general HA configuration settings. The command also displays information about how the cluster unit that you have logged into is operating in the cluster.

Usually you would log into the primary unit CLI using SSH or telnet. In this case the `get system ha status` command displays information about the primary unit first, and also displays the HA state of the primary unit (the primary unit operates in the work state). However, if you log into the primary unit and then use the `execute ha manage` command to log into a subordinate unit, (or if you use a console connection to log into a subordinate unit) the `get system status` command displays information about this subordinate unit first, and also displays the HA state of this subordinate unit. The state of a subordinate unit is work for an active-active cluster and standby for an active-passive cluster.

For a virtual cluster configuration, the `get system ha status` command displays information about how the cluster unit that you have logged into is operating in virtual cluster 1 and virtual cluster 2. For example, if you connect to the cluster unit that is the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2, the output of the `get system ha status` command shows virtual cluster 1 in the work state and virtual cluster 2 in the standby state. The `get system ha status` command also displays additional information about virtual cluster 1 and virtual cluster 2.

## Syntax

```
get system ha status
```

The command display includes the following fields. For more information see the examples that follow.

Variable	Description
Model	The FortiGate model number.
Mode	The HA mode of the cluster: a-a or a-p.
Group	The group ID of the cluster.
Debug	The debug status of the cluster.
ses_pickup	The status of session pickup: enable or disable.
load_balance	The status of the <code>load-balance-all</code> field: enable or disable. Displayed for active-active clusters only.
schedule	The active-active load balancing schedule. Displayed for active-active clusters only.
Master	<p><code>Master</code> displays the device priority, host name, serial number, and actual cluster index of the primary (or master) unit.</p> <p><code>Slave</code> displays the device priority, host name, serial number, and actual cluster index of the subordinate (or slave, or backup) unit or units.</p> <p>The list of cluster units changes depending on how you log into the CLI. Usually you would use SSH or telnet to log into the primary unit CLI. In this case the primary unit would be at the top the list followed by the other cluster units.</p> <p>If you use <code>execute ha manage</code> or a console connection to log into a subordinate unit CLI, and then enter <code>get system ha status</code> the subordinate unit that you have logged into appears at the top of the list of cluster units.</p>
number of vcluster	The number of virtual clusters. If virtual domains are not enabled, the cluster has one virtual cluster. If virtual domains are enabled the cluster has two virtual clusters.

Variable	Description
vcluster 1	<p>The HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 1. If virtual domains are not enabled, <code>vcluster 1</code> displays information for the cluster. If virtual domains are enabled, <code>vcluster 1</code> displays information for virtual cluster 1.</p> <p>The HA heartbeat IP address is 10.0.0.1 if you are logged into a the primary unit of virtual cluster 1 and 10.0.0.2 if you are logged into a subordinate unit of virtual cluster 1.</p> <p><code>vcluster 1</code> also lists the primary unit (master) and subordinate units (slave) in virtual cluster 1. The list includes the operating cluster index and serial number of each cluster unit in virtual cluster 1. The cluster unit that you have logged into is at the top of the list.</p> <p>If virtual domains are not enabled and you connect to the primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the primary unit.</p> <p>If virtual domains are not enabled and you connect to a subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you have logged into.</p> <p>If virtual domains are enabled and you connect to the virtual cluster 1 primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the virtual cluster 1 primary unit.</p> <p>If virtual domains are enabled and you connect to the virtual cluster 1 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you are logged into.</p> <p>In a cluster consisting of two cluster units operating without virtual domains enabled all clustering actually takes place in virtual cluster 1. HA is designed to work this way to support virtual clustering. If this cluster was operating with virtual domains enabled, adding virtual cluster 2 is similar to adding a new copy of virtual cluster 1. Virtual cluster 2 is visible in the <code>get system ha status</code> command output when you add virtual domains to virtual cluster 2.</p>



Variable	Description
vcluster 2	<p><code>vcluster 2</code> only appears if virtual domains are enabled.</p> <p><code>vcluster 2</code> displays the HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 2. The HA heartbeat IP address is 10.0.0.2 if you are logged into the primary unit of virtual cluster 2 and 10.0.0.1 if you are logged into a subordinate unit of virtual cluster 2.</p> <p><code>vcluster 2</code> also lists the primary unit (master) and subordinate units (slave) in virtual cluster 2. The list includes the cluster index and serial number of each cluster unit in virtual cluster 2. The cluster unit that you have logged into is at the top of the list.</p> <p>If you connect to the virtual cluster 2 primary unit CLI, the HA state of the cluster unit in virtual cluster 2 is <code>work</code>. The display lists the cluster units starting with the virtual cluster 2 primary unit.</p> <p>If you connect to the virtual cluster 2 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 2 is <code>standby</code>. The display lists the cluster units starting with the subordinate unit that you are logged into.</p>

## system info admin status

Use this command to display administrators that are logged into the FortiGate unit.

### Syntax

```
get system info admin status
```

### Example

This shows sample output.

```
Index User name Login type From
0 admin CLI ssh(172.20.120.16)
1 admin WEB 172.20.120.16
```

Variable	Description
Index	The order the administrators logged in.
User name	The name of the user account logged in.
Login type	Which interface was used to log in.
From	The IP address this user logged in from.

## Related topics

"system info admin ssh" on page 434

## system info admin ssh

Use this command to display information about the SSH configuration on the FortiGate unit such as:

the SSH port number

the interfaces with SSH enabled

the hostkey DSA fingerprint

the hostkey RSA fingerprint

### Syntax

```
get system info admin ssh
```

### Example output

```
# get system info admin ssh
SSH v2 is enabled on port 22
SSH is enabled on the following 1 interfaces:
internal
SSH hostkey DSA fingerprint = cd:e1:87:70:bb:f0:9c:7d:e3:7b:73:f7:44:23:a5:99
SSH hostkey RSA fingerprint = c9:5b:49:1d:7c:ba:be:f3:9d:39:33:4d:48:9d:b8:49
```

## system interface physical

Use this command to list information about the unit's physical network interfaces.

### Syntax

```
get system interface physical
```

The output looks like this:

```
# get system interface physical
== [onboard]
==[dmz1]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[dmz2]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[internal]
mode: static
ip: 172.20.120.146 255.255.255.0
status: up
```

```
speed: 100
==[wan1]
mode: pppoe
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[wan2]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[modem]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
```

## system ip-conflict status

List interface names and IP addresses in conflict.

### Syntax

```
get system ip-conflict status
```

## system mgmt-csum

FortiManager uses this command to obtain checksum information from FortiGate units.

### Syntax

```
get system mgmt-csum {global | vdom | all}
```

where

**global** retrieves global object checksums

**vdom** retrieves VDOM object checksums

**all** retrieves all object checksums.

## system performance firewall

Use this command to display packet distribution and traffic statistics information for the FortiGate firewall.

### Syntax

```
get system performance firewall packet-distribution
get system performance firewall statistics
```

Variable	Description
packet-distribution	<p>Display a list of packet size ranges and the number of packets of each size accepted by the firewall since the system restarted. You can use this information to learn about the packet size distribution on your network.</p> <p><b>Note:</b> these counts do not include packets offloaded to the NPU.</p>
statistics	<p>Display a list of traffic types (browsing, email, DNS etc) and the number of packets and number of payload bytes accepted by the firewall for each type since the FortiGate unit was restarted.</p>

### Example output

```

get system performance firewall packet-distribution
getting packet distribution statistics...
0 bytes - 63 bytes: 655283 packets
64 bytes - 127 bytes: 1678278 packets
128 bytes - 255 bytes: 58823 packets
256 bytes - 383 bytes: 70432 packets
384 bytes - 511 bytes: 1610 packets
512 bytes - 767 bytes: 3238 packets
768 bytes - 1023 bytes: 7293 packets
1024 bytes - 1279 bytes: 18865 packets
1280 bytes - 1500 bytes: 58193 packets
> 1500 bytes: 0 packets

get system performance firewall statistics
getting traffic statistics...
Browsing: 623738 packets, 484357448 bytes
DNS: 5129187383836672 packets, 182703613804544 bytes
E-Mail: 23053606 packets, 2 bytes
FTP: 0 packets, 0 bytes
Gaming: 0 packets, 0 bytes
IM: 0 packets, 0 bytes
Newsgroups: 0 packets, 0 bytes
P2P: 0 packets, 0 bytes
Streaming: 0 packets, 0 bytes
TFTP: 654722117362778112 packets, 674223966126080 bytes
VoIP: 16834455 packets, 10 bytes
Generic TCP: 266287972352 packets, 8521215115264 bytes
Generic UDP: 0 packets, 0 bytes
Generic ICMP: 0 packets, 0 bytes
Generic IP: 0 packets, 0 bytes

```

## system performance status

Use this command to display FortiGate CPU usage, memory usage, network usage, sessions, virus, IPS attacks, and system up time.

## Syntax

```
get system performance status
```

Variable	Description
CPU states	<p>The percentages of CPU cycles used by user, system, nice and idle categories of processes. These categories are:</p> <p><code>user</code> -CPU usage of normal user-space processes</p> <p><code>system</code> -CPU usage of kernel</p> <p><code>nice</code> - CPU usage of user-space processes having other-than-normal running priority</p> <p><code>idle</code> - Idle CPU cycles</p> <p>Adding user, system, and nice produces the total CPU usage as seen on the CPU widget on the web-based system status dashboard.</p>
Memory states	The percentage of memory used.
Average network usage	The average amount of network traffic in kbps in the last 1, 10 and 30 minutes.
Average sessions	The average number of sessions connected to the FortiGate unit over the last 1, 10 and 30 minutes.
Virus caught	The number of viruses the FortiGate unit has caught in the last 1 minute.
IPS attacks blocked	The number of IPS attacks that have been blocked in the last 1 minute.
Uptime	How long since the FortiGate unit has been restarted.

## Example output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
Memory states: 18% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 1 kbps in 30 minutes
Average sessions: 5 sessions in 1 minute, 6 sessions in 10 minutes, 5 sessions in 30
minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 9days, 22 hours, 0 minutes
```

## system performance top

Use this command to display the list of processes running on the FortiGate unit (similar to the Linux `top` command).

You can use the following commands when `get system performance top` is running:

- Press Q or Ctrl+C to quit.
- Press P to sort the processes by the amount of CPU that the processes are using.
- Press M to sort the processes by the amount of memory that the processes are using.

## Syntax

```
get system performance top [<delay_int>] <max_lines_int>]]
```

Variable	Description
<delay_int>	The delay, in seconds, between updating the process list. The default is 5 seconds.
<max_lines_int>	The maximum number of processes displayed in the output. The default is 20 lines.

## system session list

Command returns a list of all the sessions active on the FortiGate unit. or the current virtual domain if virtual domain mode is enabled.

## Syntax

```
get system session list
```

## Example output

PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT
tcp	0	127.0.0.1:1083 -	127.0.0.1:514 -		
tcp	0	127.0.0.1:1085 -	127.0.0.1:514 -		
tcp	10	127.0.0.1:1087 -	127.0.0.1:514 -		
tcp	20	127.0.0.1:1089 -	127.0.0.1:514 -		
tcp	30	127.0.0.1:1091 -	127.0.0.1:514 -		
tcp	40	127.0.0.1:1093 -	127.0.0.1:514 -		
tcp	60	127.0.0.1:1097 -	127.0.0.1:514 -		
tcp	70	127.0.0.1:1099 -	127.0.0.1:514 -		
tcp	80	127.0.0.1:1101 -	127.0.0.1:514 -		
tcp	90	127.0.0.1:1103 -	127.0.0.1:514 -		
tcp	100	127.0.0.1:1105 -	127.0.0.1:514 -		
tcp	110	127.0.0.1:1107 -	127.0.0.1:514 -		
tcp	103	172.20.120.16:3548 -	172.20.120.133:22 -		
tcp	3600	172.20.120.16:3550 -	172.20.120.133:22 -		
udp	175	127.0.0.1:1026 -	127.0.0.1:53 -		
tcp	5	127.0.0.1:1084 -	127.0.0.1:514 -		
tcp	5	127.0.0.1:1086 -	127.0.0.1:514 -		
tcp	15	127.0.0.1:1088 -	127.0.0.1:514 -		
tcp	25	127.0.0.1:1090 -	127.0.0.1:514 -		
tcp	45	127.0.0.1:1094 -	127.0.0.1:514 -		
tcp	59	127.0.0.1:1098 -	127.0.0.1:514 -		
tcp	69	127.0.0.1:1100 -	127.0.0.1:514 -		
tcp	79	127.0.0.1:1102 -	127.0.0.1:514 -		

```
tcp 99 127.0.0.1:1106 -      127.0.0.1:514 -
tcp 109 127.0.0.1:1108 -     127.0.0.1:514 -
tcp 119 127.0.0.1:1110 -     127.0.0.1:514 -
```

Variable	Description
PROTO	The transfer protocol of the session.
EXPIRE	How long before this session will terminate.
SOURCE	The source IP address and port number.
SOURCE-NAT	The source of the NAT. '-' indicates there is no NAT.
DESTINATION	The destination IP address and port number.
DESTINATION-NAT	The destination of the NAT. '-' indicates there is no NAT.

## system session status

Use this command to display the number of active sessions on the FortiGate unit, or if virtual domain mode is enabled it returns the number of active sessions on the current VDOM. In both situations it will say 'the current VDOM'.

### Syntax

```
get system session status
```

### Example output

```
The total number of sessions for the current VDOM: 3100
```

## system session-helper-info list

Use this command to list the FortiGate session helpers and the protocol and port number configured for each one.

### Syntax

```
get system session-helper-info list
```

### Example output

```
list builtin help module:
mgcp
dcerpc
rsh
pmap
dns-tcp
dns-udp
rtsp
pptp
```

```

sip
mms
tns
h245
h323
ras
tftp
ftp
list session help:
help=pmap, protocol=17 port=111
help=rtsp, protocol=6 port=8554
help=rtsp, protocol=6 port=554
help=pptp, protocol=6 port=1723
help=rtsp, protocol=6 port=7070
help=sip, protocol=17 port=5060
help=pmap, protocol=6 port=111
help=rsh, protocol=6 port=512
help=dns-udp, protocol=17 port=53
help=tftp, protocol=17 port=69
help=tns, protocol=6 port=1521
help=mgcp, protocol=17 port=2727
help=dcerpc, protocol=17 port=135
help=rsh, protocol=6 port=514
help=ras, protocol=17 port=1719
help=ftp, protocol=6 port=21
help=mgcp, protocol=17 port=2427
help=dcerpc, protocol=6 port=135
help=mms, protocol=6 port=1863
help=h323, protocol=6 port=1720

```

## system session-info

Use this command to display session information.

### Syntax

```

get system session-info expectation
get system session-info full-stat
get system session-info list
get system session-info statistics
get system session-info ttl

```

Variable	Description
expectation	Display expectation sessions.
full-stat	Display detailed information about the FortiGate session table including a session table and expect session table summary, firewall error statistics, and other information.



Variable	Description
list	Display detailed information about all current FortiGate sessions. For each session the command displays the protocol number, traffic shaping information, policy information, state information, statistics and other information.
statistics	Display the same information as the <code>full-stat</code> command except for the session table and expect session table summary.
ttl	Display the current setting of the <code>config system session-ttl</code> command including the overall session timeout as well as the timeouts for specific protocols.

### Example output

```
get system session-info statistics
misc info: session_count=15 exp_count=0 clash=0 memory_tension_drop=0 ephemeral=1/32752
           removeable=14
delete=0, flush=0, dev_down=0/0
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000001
tcp reset stat:
syncqf=0 acceptqf=0 no-listener=227 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

## system source-ip

Use this command to list defined source-IPs.

### Syntax

```
get system source-ip
```

### Example output

```
# get sys source-ip status
The following services force their communication to use
a specific source IP address:

service=NTP source-ip=172.18.19.101
service=DNS source-ip=172.18.19.101
vdom=root service=RADIUS name=server-pc25 source-ip=10.1.100.101
vdom=root service=TACACS+ name=tac_plus_pc25 source-ip=10.1.100.101
```

```
vdom=root service=FSAE name=pc26 source-ip=172.18.19.101
vdom=V1 service=RADIUS name=pc25-Radius source-ip=172.16.200.101
vdom=V1 service=TACACS+ name=pc25-tacacs+ source-ip=172.16.200.101
vdom=V1 service=FSAE name=pc16 source-ip=172.16.200.101
```

## system startup-error-log

Use this command to display information about system startup errors. This command only displays information if an error occurs when the FortiGate unit starts up.

### Syntax

```
get system startup-error-log
```

## system stp list

Use this command to display Spanning Tree Protocol status.

### Syntax

```
get system stp list
```

## system status

Use this command to display system status information including:

FortiGate firmware version, build number and branch point

virus and attack definitions version

FortiGate unit serial number and BIOS version

log hard disk availability

host name

operation mode

virtual domains status: current VDOM, max number of VDOMs, number of NAT and TP mode VDOMs and VDOM status

current HA status

system time

the revision of the WiFi chip in a FortiWiFi unit

### Syntax

```
get system status
```

## Example output

```
Version: Fortigate-620B v4.0,build0271,100330 (MR2)
Virus-DB: 11.00643(2010-03-31 17:49)
Extended DB: 11.00643(2010-03-31 17:50)
Extreme DB: 0.00000(2003-01-01 00:00)
IPS-DB: 2.00778(2010-03-31 12:55)
FortiClient application signature package: 1.167(2010-04-01 10:11)
Serial-Number: FG600B3908600705
BIOS version: 04000006
Log hard disk: Available
Hostname: 620_ha_1
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Distribution: International
Branch point: 271
Release Version Information: MR2
System time: Thu Apr 1 15:27:29 2010
```

## test

Use this command to display information about FortiGate applications and perform operations on FortiGate applications. You can specify an application name and a test level. Enter ? to display the list of applications. The test level performs various functions depending on the application but can include displaying memory usage, dropping connections and restarting the application.

The test levels are different for different applications. In some cases when you enter the command and include an application name but no test level (or an invalid test level) the command output includes a list of valid test levels.

## Syntax

```
get test <application_name_str> <test_level_int>
```

## Example output

```
get test http
Proxy Worker 0 - http
[0:H] HTTP Proxy Test Usage
[0:H]
[0:H] 2: Drop all connections
[0:H] 22: Drop max idle connections
[0:H] 222: Drop all idle connections
[0:H] 4: Display connection stat
[0:H] 44: Display info per connection
[0:H] 444: Display connections per state
[0:H] 4444: Display per-VDOM statistics
[0:H] 44444: Display information about idle connections
[0:H] 55: Display tcp info per connection
```

```
get test http 4
HTTP Common
Current Connections 0/8032

HTTP Stat
Bytes sent 0 (kb)
Bytes received 0 (kb)
Error Count (alloc) 0
Error Count (accept) 0
Error Count (bind) 0
Error Count (connect) 0
Error Count (socket) 0
Error Count (read) 0
Error Count (write) 0
Error Count (retry) 0
Error Count (poll) 0
Error Count (scan reset) 0
Error Count (urlfilter wait) 0
Last Error 0
Web responses clean 0
Web responses scan errors 0
Web responses detected 0
Web responses infected with worms 0
Web responses infected with viruses 0
Web responses infected with susp 0
Web responses file blocked 0
Web responses file exempt 0
Web responses bannedword detected 0
Web requests oversize pass 0
Web requests oversize block 0
URL requests exempt 0
URL requests blocked 0
URL requests passed 0
URL requests submit error 0
URL requests rating error 0
URL requests rating block 0
URL requests rating allow 0
URL requests infected with worms 0
Web requests detected 0
Web requests file blocked 0
Web requests file exempt 0
POST requests clean 0
POST requests scan errors 0
POST requests infected with viruses 0
POST requests infected with susp 0
POST requests file blocked 0
POST requests bannedword detected 0
POST requests oversize pass 0
POST requests oversize block 0
Web request backlog drop 0
Web response backlog drop 0

HTTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
urlfilter=0/0/0 uf_lookupf=0
scan=0 clt=0 srv=0
```

## user adgrp

Use this command to list Directory Service user groups.

### Syntax

```
get user adgrp [<dsgroupname>]
```

If you do not specify a group name, the command returns information for all Directory Service groups. For example:

```
== [ DOCTEST/Cert Publishers ]
name: DOCTEST/Cert Publishers server-name: DSserv1
== [ DOCTEST/Developers ]
name: DOCTEST/Developers server-name: DSserv1
== [ DOCTEST/Domain Admins ]
name: DOCTEST/Domain Admins server-name: DSserv1
== [ DOCTEST/Domain Computers ]
name: DOCTEST/Domain Computers server-name: DSserv1
== [ DOCTEST/Domain Controllers ]
name: DOCTEST/Domain Controllers server-name: DSserv1
== [ DOCTEST/Domain Guests ]
name: DOCTEST/Domain Guests server-name: DSserv1
== [ DOCTEST/Domain Users ]
name: DOCTEST/Domain Users server-name: DSserv1
== [ DOCTEST/Enterprise Admins ]
name: DOCTEST/Enterprise Admins server-name: DSserv1
== [ DOCTEST/Group Policy Creator Owners ]
name: DOCTEST/Group Policy Creator Owners server-name: DSserv1
== [ DOCTEST/Schema Admins ]
name: DOCTEST/Schema Admins server-name: DSserv1
```

If you specify a Directory Service group name, the command returns information for only that group. For example:

```
name : DOCTEST/Developers
server-name : ADServ1
```

The `server-name` is the name you assigned to the Directory Service server when you configured it in the `user fsae` command.

## vpn certificate

Display detailed information about local and CA certificates installed on the FortiGate. This is a VDOM level command. The global command is `get certificate`.

### Syntax

```
get vpn certificate {local | ca} details [certificate_name]
```

## vpn ike gateway

Use this command to display information about FortiGate IPsec VPN IKE gateways.

### Syntax

```
get vpn ike gateway [<gateway_name_str>]
```

## vpn ipsec tunnel details

Use this command to display detailed information about IPsec tunnels.

### Syntax

```
get vpn ipsec tunnel details
```

## vpn ipsec tunnel name

Use this command to display information about a specified IPsec VPN tunnel.

### Syntax

```
get vpn ipsec tunnel name <tunnel_name_str>
```

## vpn ipsec tunnel summary

Use this command to display summary information about IPsec tunnels.

### Syntax

```
get vpn ipsec tunnel summary
```

## vpn ipsec stats crypto

Use this command to display information about the FortiGate hardware and software crypto configuration.

### Syntax

```
get vpn ipsec stats crypto
```

### Example output

```
get vpn ipsec stats crypto

IPsec crypto devices in use:
```

```
CP6 (encrypted/decrypted):
  null:  0      0
  des:    0      0
  3des:   0      0
  aes:    0      0
CP6 (generated/validated):
  null:  0      0
  md5:    0      0
  sha1:   0      0
  sha256: 0      0

SOFTWARE (encrypted/decrypted):
  null:  0      0
  des:    0      0
  3des:   0      0
  aes:    0      0
SOFTWARE (generated/validated):
  null:  0      0
  md5:    0      0
  sha1:   0      0
  sha256: 0      0
```

## vpn ipsec stats tunnel

Use this command to view information about IPsec tunnels.

### Syntax

```
get vpn ipsec stats tunnel
```

### Example output

```
#get vpn ipsec stats tunnel
tunnels
total: 0
static/ddns: 0
dynamic: 0
manual: 0
errors: 0
selectors
total: 0
up: 0
```

## vpn ssl monitor

Use this command to display information about logged in SSL VPN users and current SSL VPN sessions.

## Syntax

```
get vpn ssl monitor
```

## Example output

## vpn status l2tp

Use this command to display information about L2TP tunnels.

## Syntax

```
get vpn status l2tp
```

## vpn status pptp

Use this command to display information about PPTP tunnels.

## Syntax

```
get vpn status pptp
```

## vpn status ssl

Use this command to display SSL VPN tunnels and to also verify that the FortiGate unit includes the CP6 or greater FortiASIC device that supports SSL acceleration.

## Syntax

```
get vpn status ssl hw-acceleration-status  
get vpn status ssl list
```

Variable	Description
hw-acceleration-status	Display whether or not the FortiGate unit contains a FortiASIC device that supports SSL acceleration.
list	Display information about all configured SSL VPN tunnels.

## webfilter categories

List the FortiGuard Web Filtering categories.



## Syntax

```
get webfilter categories
```

## Example output (partial)

```
FG-5KD3914800284 # get webfilter categories
```

```
g01 Potentially Liable:
  1 Drug Abuse
  3 Hacking
  4 Illegal or Unethical
  5 Discrimination
  6 Explicit Violence
 12 Extremist Groups
 59 Proxy Avoidance
 62 Plagiarism
 83 Child Abuse
g02 Adult/Mature Content:
  2 Alternative Beliefs
  7 Abortion
  8 Other Adult Materials
  9 Advocacy Organizations
 11 Gambling
 13 Nudity and Risque
 14 Pornography
 15 Dating
 16 Weapons (Sales)
 57 Marijuana
 63 Sex Education
 64 Alcohol
 65 Tobacco
 66 Lingerie and Swimsuit
 67 Sports Hunting and War Games
g04 Bandwidth Consuming:
 19 Freeware and Software Downloads
 24 File Sharing and Storage
 25 Streaming Media and Download
 72 Peer-to-peer File Sharing
 75 Internet Radio and TV
 76 Internet Telephony
g05 Security Risk:
 26 Malicious Websites
 61 Phishing
 86 Spam URLs
 88 Dynamic DNS
    ...
```

## webfilter ftgd-statistics

Use this command to display FortiGuard Web Filtering rating cache and daemon statistics.

## Syntax

```
get webfilter ftgd-statistics
```

## Example output

```
get webfilter ftgd-statistics

Rating Statistics:
=====
DNS failures : 0
DNS lookups : 0
Data send failures : 0
Data read failures : 0
Wrong package type : 0
Hash table miss : 0
Unknown server : 0
Incorrect CRC : 0
Proxy request failures : 0
Request timeout : 0
Total requests : 0
Requests to FortiGuard servers : 0
Server errored responses : 0
Relayed rating : 0
Invalid profile : 0

Allowed : 0
Blocked : 0
Logged : 0
Errors : 0

Cache Statistics:
=====
Maximum memory : 0
Memory usage : 0

Nodes : 0
Leaves : 0
Prefix nodes : 0
Exact nodes : 0

Requests : 0
Misses : 0
Hits : 0
Prefix hits : 0
Exact hits : 0

No cache directives : 0
Add after prefix : 0
Invalid DB put : 0
DB updates : 0

Percent full : 0%
Branches : 0%
Leaves : 0%
Prefix nodes : 0%
```

```
Exact nodes : 0%
```

```
Miss rate : 0%
```

```
Hit rate : 0%
```

```
Prefix hits : 0%
```

```
Exact hits : 0%
```

## webfilter status

Use this command to display FortiGate Web Filtering rating information.

### Syntax

```
get webfilter status [<refresh-rate_int>]
```

## wireless-controller client-info

Use this command to get information about WiFi clients.

### Syntax

```
get wireless-controller client-info <vfid> <interface> <client_ip>
```

The output looks like this:

```
# get wireless-controller client-info 0 test-local 192.168.2.100
count=1
status: sta_mac=10:fe:ed:26:aa:e0 ap_sn=FP320C3X14006184, ap_name=FP320C3X14006184,
       chan=6, radio_type=11N
```

## wireless-controller rf-analysis

Use this command to show information about RF conditions at the access point.

### Syntax

```
get wireless-controller rf-analysis [<wtp_id>]
```

### Example output

```
# get wireless-controller rf-analysis
<wtp-id> wtp id

FWF60C3G11004319 (global) # get wireless-controller rf-analysis
WTP: FWF60C-WIFI0 0-127.0.0.1:15246
channel rssi-total rf-score overlap-ap interfere-ap
1 418 1 24 26
2 109 5 0 34
3 85 7 1 34
4 64 9 0 35
```

```

5 101 6 1 35
6 307 1 8 11
7 82 7 0 16
8 69 8 1 15
9 42 10 0 15
10 53 10 0 14
11 182 1 5 6
12 43 10 0 6
13 20 10 0 5
14 8 10 0 5
Controller: FWF60C3G11004319-0
channel rssi_total
1 418
2 109
3 85
4 64
5 101
6 307
7 82
8 69
9 42
10 53
11 182
12 43
13 20
14 8

```

## wireless-controller scan

Use this command to view the list of access points detected by wireless scanning.

### Syntax

```
get wireless-controller scan
```

### Example output

CMW	SSID	BSSID	CHAN	RATE	S:N	INT	CAPS	ACT	LIVE	AGE	WIRED
UNN		00:0e:8f:24:18:6d	64	54M	16:0	100	Es	N	62576	1668	?
UNN	ftiguest	00:15:55:23:d8:62	157	130M	6:0	100	EPs	N	98570	2554	?

## wireless-controller spectral-info

Use this command to display wireless controller spectrum analysis.

### Syntax

```
get wireless-controller spectral-info
```

## wireless-controller status

Use this command to view the numbers of wtp sessions and clients.

### Syntax

```
get wireless-controller status
```

### Example output

```
# get wireless-controller status
Wireless Controller :
wtp-session-count: 1
client-count : 1/0
```

## wireless-controller vap-status

Use this command to view information about your SSIDs.

### Syntax

```
get wireless-controller vap-status
```

### Example output

```
# get wireless-controller vap-status
WLAN: mesh.root
name : mesh.root
vdom : root
ssid : fortinet.mesh.root
status : up
mesh backhaul : yes
ip : 0.0.0.0
mac : 00:ff:0a:57:95:ca
station info : 0/0
WLAN: wifi
name : wifi
vdom : root
ssid : ft-mesh
status : up
mesh backhaul : yes
ip : 10.10.80.1
mac : 00:ff:45:e1:55:81
station info : 1/0
```

## wireless-controller wlchanlistlic

Use this command to display a list of the channels allowed in your region, including the maximum permitted power for each channel

the channels permitted for each wireless type (802.11n, for example)

The list is in XML format.

## Syntax

```
get wireless-controller wlchanlistlic
```

## Sample output

```
country name: UNITED STATES2, country code:841, iso name:US
channels on 802.11A band without channel bonding:
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=165 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11B band without channel bonding:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11G band without channel bonding:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11N 2.4GHz band without channel bonding:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

```
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

```
channels on 802.11N 2.4GHz band with channel bonding plus:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

```
channels on 802.11N 2.4GHz band with channel bonding minus:
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

```
channels on 802.11N 5GHz band without channel bonding:
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=165 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
```

```
channels on 802.11N 5GHz band with channel bonding all:
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
```

## wireless-controller wtp-status

### Syntax

```
get wireless-controller wtp-status
```

### Example output

```
# get wireless-controller wtp-status
```

```
WTP: FAP22B3U11005354 0-192.168.3.110:5246
wtp-id : FAP22B3U11005354
region-code :
name :
mesh-uplink : mesh
mesh-downlink : disabled
mesh-hop-count : 1
parent-wtp-id :
software-version :
local-ipv4-addr : 0.0.0.0
board-mac : 00:00:00:00:00:00
join-time : Mon Apr 2 10:23:32 2012
connection-state : Disconnected
image-download-progress: 0
last-failure : 0 -- N/A
last-failure-param:
last-failure-time: N/A
Radio 1 : Monitor
Radio 2 : Ap
country-name : NA
country-code : N/A
client-count : 0
base-bssid : 00:00:00:00:00:00
max-vaps : 7
oper-chan : 0
Radio 3 : Not Exist
WTP: FWF60C-WIFI0 0-127.0.0.1:15246
wtp-id : FWF60C-WIFI0
region-code : ALL
name :
mesh-uplink : ethernet
mesh-downlink : enabled
mesh-hop-count : 0
parent-wtp-id :
software-version : FWF60C-v5.0-build041
local-ipv4-addr : 127.0.0.1
board-mac : 00:09:0f:fe:cc:56
join-time : Mon Apr 2 10:23:35 2012
connection-state : Connected
image-download-progress: 0
last-failure : 0 -- N/A
last-failure-param:
last-failure-time: N/A
Radio 1 : Ap
country-name : US
country-code : N/A
client-count : 1
base-bssid : 00:0e:8e:3b:63:99
max-vaps : 7
oper-chan : 1
Radio 2 : Not Exist
Radio 3 : Not Exist
```



## tree

The `tree` command displays FortiOS `config` CLI commands in a tree structure called the configuration tree. Each configuration command forms a branch of the tree.

### Syntax

```
tree [branch] [sub-branch]
```

You can enter the `tree` command from the top of the configuration tree the command displays the complete configuration tree. Commands are displayed in the order that they are processed when the FortiGate unit starts up. For example, the following output shows the first 10 lines of `tree` command output:

```
tree
-- -- system -- [vdom] --*name (12)
+- vcluster-id (0,0)
|- <global> -- language
|- gui-ipv6
|- gui-voip-profile
|- gui-lines-per-page (20,1000)
|- admintimeout (0,0)
|- admin-concurrent
|- admin-lockout-threshold (0,0)
|- admin-lockout-duration (1,2147483647)
|- refresh (0,2147483647)
|- interval (0,0)
|- failtime (0,0)
|- daily-restart
|- restart-time
...
```

You can include a branch name with the `tree` command to view the commands in that branch:

```
tree user
-- user -- [radius] --*name (36)
    |- server (64)
    |- secret
    |- secondary-server (64)
    |- secondary-secret
    ...
    |- [tacacs+] --*name (36)
        |- server (64)
        |- secondary-server (64)
        |- tertiary-server (64)
        ...
    |- [ldap] --*name (36)
        |- server (64)
        |- secondary-server (64)
        |- tertiary-server (64)
        |- port (1,65535)
        ...
```

You can include a branch and sub branch name with the `tree` command to view the commands in that sub branch:

```
tree user local
-- [local] --*name (36)
|- status
```

```

|- type
|- passwd
|- ldap-server (36)
|- radius-server (36)
+- tacacs+-server (36)

```

...

If you enter the `tree` command from inside the configuration `tree` the command displays the tree for the current command:

```

config user ldap
tree
-- [ldap] --*name (36)
|- server (64)
|- cnid (21)
|- dn (512)
|- port (1,65535)
|- type

```

...

The `tree` command output includes information about field limits. These apply in both the CLI and the web-based manager. For a numeric field, the two numbers in parentheses show the lower and upper limits. For example (0,32) indicates that values from 0 to 32 inclusive are accepted. For string values, the number in parentheses is one more than the maximum number of characters permitted.

In the following example, the FQDN can contain up to 255 characters.

```

config firewall address
tree
-- [address] --*name (64)
    |- subnet
    |- type
    |- start-ip
    |- end-ip
    |- fqdn (256)
    |- country (3)
    |- cache-ttl (0,86400)
    |- wildcard
    |- comment
    |- visibility
    |- associated-interface (36)
    |- color (0,32)
+- [tags] --*name (64)

```



**FORTINET®**

High Performance Network Security



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.